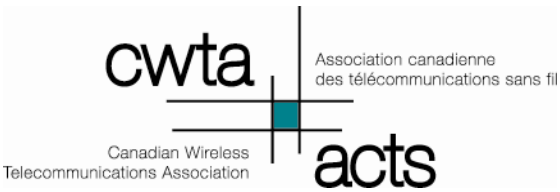


Comparison of International Handset Security Measures

August 13, 2012

Contents

1. Background

As smartphones increase in capability – and value – an increasing amount of attention is being focused on handset theft, including growing opinion that network operators and telecommunications regulators should play a role in deterring handset theft. Specifically, some politicians and law enforcement officials believe a database shared between operators to ensure phones reported stolen or lost are not activated on another network will eliminate the domestic market for stolen handsets, and therefore greatly reduce handset theft.

Such an approach has been instituted in a number of countries globally, as well as on an international level, although not to the extent indicated in recent media reports in Canada and the US. It appears that the UK and Australia are the only countries that have been using an industry-wide IMEI (International Mobile Equipment Identity) database to block stolen and lost phones for more than a decade. While statistics from those countries indicate that Industry-wide IMEI databases reduce handset theft, they are far from a panacea.

IMEI databases can only be considered part of a solution. Comprehensive efforts to curtail handset theft also include cooperation from law enforcement agencies, public awareness campaigns and appropriate legislation that makes it illegal to change IMEI numbers or to reactivate a handset reported as lost or stolen. Indeed, network operators in France established a shared IMEI database in 2003, but legislation banning the activation of a stolen phone was only instituted in 2011.

Handset theft is still significant in the countries (the UK and Australia in particular) with the most comprehensive theft-reduction measures. While a particular jurisdiction can reduce the market for stolen phones within its own borders, it cannot do so in other parts of the world. There is significant global demand for black market cell phones.

The UK's Mobile Crime Industry Action Forum (MICAF) reported that in 2004 black market handsets accounted for:

- 90% of handsets sold in Russia;
- 85% of the handsets sold in Ukraine;
- 66% of handsets sold in Central and Eastern Europe; and

- 27% of handsets sold in Africa and the Middle East.[1]

Outside markets for stolen handsets will ensure that handset theft remains an issue in virtually every country. This report examines measures in place globally and indicates their impact to date.

2. GSMA – IMEI Database[2] and Blacklist Sharing

The GSM Association maintains an IMEI (International Mobile Equipment Identity) Database to help deter cell phone theft and its consequences. The association has been operating the database since 1996.

The Blacklist

The IMEI Database supports a 'black list' of IMEIs that are associated with devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use.

Blacklist Sharing

Because it is a central system, the IMEI Database allows network operators to share their individual black lists so that devices denied service (blacklisted) by one network will not work on other networks even if the SIM card in the device is changed.

Network operators who deploy Equipment Identity Register (EIR) in their networks use them to keep their own lists of blacklisted lost or stolen phones. Operators' EIRs automatically connect to the IMEI Database system to share their latest lists of blacklisted devices with other operators.

Every day since 1996, the IMEI Database has taken all the black lists from different operators around the world and added them together into one global black list. When an EIR subsequently connects to the IMEI Database, it downloads the latest global black list (or a national or regional subset of the global list) for its own use. By loading the IMEI Database black list onto the local EIR, all handsets reported as stolen on other connected networks up to the previous day are now also blocked on that network.

The GSMA's IMEI Database solution is provided free of charge to GSMA members. The IMEI Database is designed to act as a global repository of handset data to which GSMA member operators can connect to submit and obtain data. It is the most widely used handset data sharing platform and ensures that the mobile phones reported as stolen in one country will not work in other countries that have signed up to use the Database.

Global Participation

Currently, 50 operators from 24 different countries are connected to the IMEI Database and sharing their blacklist daily. The table below lists the operators, their country of operation, and the date they joined the IMEI Database.

[1] Mobile Industry Crime Action Forum, Presentation: *Tackling Mobile Phone Theft in the UK*, 2009.
[2] http://www.gsma.com/publicpolicy/handset-theft/

Table 1: Operators connected to the GSMA's IMEI Database (and date of connection)[3][4]

Operator	Country	Date Connected
TDC Mobil A/S	Denmark	25-Dec-2004
DNA Oy	Finland	25-Dec-2004
Cyprus Telecommunications Auth	Cyprus	25-Dec-2004
Vodafone Malta Limited	Malta	25-Dec-2004
Telenor Sverige AB	Sweden	25-Dec-2004
T-Mobile (UK) Limited	United Kingdom	25-Dec-2004
Telenor Mobile	Norway	25-Dec-2004
TeliaSonera Mobile Networks AB	Sweden	25-Dec-2004
Vodafone Omnitel N.V.	Italy	25-Dec-2004
Belgacom Mobile	Belgium	25-Dec-2004
Tele 2 AB	Sweden	25-Dec-2004
Orange PCS Ltd	United Kingdom	25-Dec-2004
Telecom Italia Mobile	Italy	25-Dec-2004
Vodafone Egypt Telecommunications S.A.E	Egypt	25-Dec-2004
Sonera Mobile Networks Limited	Finland	25-Dec-2004
VODAFONE Ltd	United Kingdom	25-Dec-2004
Pannon GSM Telecommunications	Hungary	25-Dec-2004
Celtel Kenya Ltd.	Kenya	25-Dec-2004
NetCom AS	Norway	25-Dec-2004
Wind Telecomunicazioni SpA	Italy	25-Dec-2004
Hutchison 3G UK Ltd	United Kingdom	25-Dec-2004
Meteor Mobile Telecommunications Limited	Ireland	25-Dec-2004
Mobistar S.A.	Belgium	25-Dec-2004
Vodafone Espana S.A.	Spain	25-Dec-2004
O2 Ireland	Ireland	25-Dec-2004
Vodacom Group Pvt Ltd.	South Africa	25-Dec-2004
AS EMT	Estonia	25-Dec-2004
BASE NV/SA	Belgium	25-Dec-2004
H3G	Italy	25-Dec-2004
Vodafone Portugal	Portugal	25-Dec-2004

[3] Source: GSMA. Note: the IMEI Database adopted a new platform in December 2004 and no longer has records of when participants who were connected prior to that date originally connected to the previous platform. Therefore, all operators listed as being connected on December 25, 2004 were connected prior to that date.

[4] Table 1 lists all operators who currently make available the blacklist of phones on their network reported lost or stolen. However, operators connected to the IMEI Database can choose which other operators to upload lost/stolen phone information from, and whether or not to use that information to block phones on their networks. Therefore, any operator connected to the database is not necessarily uploading lost/stolen phone info from all other operators, or using uploaded information to block phones on its network.

O2 (UK) Limited	United Kingdom	25-Dec-2004
Telia A/S Denmark	Denmark	25-Dec-2004
Vodafone D2 GmbH	Germany	9-Feb-2005
Bouygues Telecom	France	9-Feb-2005
Orange France	France	9-Feb-2005
SFR - CEGETEL	France	9-Feb-2005
Telefonica O2 Czech Republic, a.s.	Czech Republic	22-Jun-2005
ICE Costa Rica	Costa Rica	18-Jul-2005
Hutchison 3G Ireland limited	Ireland	1-Aug-2005
Vodafone Hungary Ltd.	Hungary	5-Sep-2005
Movistar Chile	Chile	8-Nov-2005
Vodafone Ireland Ltd	Ireland	9-Nov-2005
Hi3G Access AB	Sweden	28-Nov-2007
Cable & Wireless UK Ltd.	United Kingdom	9-Feb-2009
Sonofon	Denmark	18-Jan-2010
Etisalat - Emirates Telecommunications Corporation	United Arab Emirates	7-Feb-2011
Corporacion Digitel C.A.	Venezuela	18-Oct-2011
CLARO CR TELECOMUNICACIONES	Costa Rica	7-Feb-2012
Emirates Integrated Telecommunications Company, PJSC	United Arab Emirates	8-May-2012
Telefonica de Costa Rica TC	Costa Rica	18-May-2012

An additional 26 network operators globally have activated IMEI Database test accounts in the past with the GSMA, but have not yet fully connected to the database.

Table 2: Operators with IMEI Database test accounts and date of test account activation

Operator	Country	Activation Date
Elisa Corporation	Finland	25-Dec-2004
Vodafone-Panafon	Greece	25-Dec-2004
Vodafone Netherlands	Netherlands	31-Aug-2005
Saudi Telecom Company (STC)	Saudi Arabia	18-Oct-2005
Telefonica Moviles Espa¿a	Spain	5-May-2006
MTN Ghana	Ghana	6-Jun-2006
Millicom Ghana Limited	Ghana	15-Mar-2007
Swisscom Mobile Ltd	Switzerland	27-Mar-2007
Tusmobil d.o.o	Slovenia	5-Jul-2007
Ghana Telecommunications Ltd	Ghana	4-Mar-2008
Orange Communications SA	Switzerland	3-Jun-2008
MTU Nett AS	Norway	9-Sep-2008
Zain Telecommunications Ghana Ltd.	Ghana	31-Oct-2008
Rogers Wireless Inc.	Canada	9-Jan-2009

Belgacom Test Account	Belgium	22-May-2009
Uralsvyazinform	Russian Federation	17-Jul-2009
HUAWEI	China	21-Jul-2009
BSNL	India	4-Aug-2009
Mahanagar Telephone Nigam Ltd, Mumbai	India	14-Dec-2009
ESSAR TELECOM KENYA LIMITED	Kenya	15-Mar-2010
Telecomunicaciones Movilnet C.A.	Venezuela	1-Jun-2010
Free Mobile	France	9-Sep-2011
T-Mobile USA, Inc	United States	16-May-2011
Telecom Personal SA	Argentina	16-Jul-2012
Telefonica Moviles El Salvador, S.A de c.v	El Salvador	27-Jul-2012
Telefonica Celular de Nicaragua	Nicaragua	29-Jul-2012

National Participation

IMEI black lists should in theory be more effective when there is greater buy-in from all carriers, thereby limiting options for lost and stolen handsets to be reactivated within the same country. The table below notes the level national participation in the IMEI black list by providing the combined subscriber share of the connected operators in each of the 24 countries that have some participation in the database.[5]

Table 3: Levels of national participation in GSMA's IMEI Database[6]

Country	Connected Operators	% Subscriber Share
United Kingdom	6	100%
Sweden	4	100%
Italy	4	100%
France	3	100%
Belgium	3	100%
Ireland	4	100%
Costa Rica	3	100%
UAE	2	100%
Denmark	3	86%
Norway	2	82%
Finland	2	60%
Hungary	2	53%
Malta	1	56%
South Africa	1	50%
Cyprus	1	50%

[5] Subscriber information was not available for all countries participating.
[6] Source: GSMA; Bank of America Merrill Lynch, *Global Wireless Matrix*, Q1 2012.

Country	Connected Operators	% Subscriber Share
Estonia	1	43%
Chile	1	39%
Egypt	1	37%
Czech Republic	1	36%
Portugal	1	36%
Germany	1	33%
Spain	1	30%
Venezuela	1	23%
Kenya	1	16%

As the table illustrates above, eight countries – UK, Sweden, Italy, Belgium, France, UAE, Ireland and Costa Rica – have all operators participating in the IMEI Database, with a ninth – Denmark – having near full participation. The remaining Scandinavian countries also each have more than 60% of subscribers connected to the IMEI Database.

Participation in the shared IMEI Databases in the European Community is not yet absolute. Specifically, Spain (30% of subscribers connected), Germany (33%), Portugal (36%), Czech Republic (36%), the Netherlands (0%), Poland (0%), Austria (0%), Switzerland (0%) and Greece (0%) have limited or no participation.

GSMA's IMEI Database vs. National Database

As it will be described in this study, some countries report implementing national shared databases for stolen handsets among all operators, even though all of their operators have also joined the GSMA's IMEI Database. By doing so, the wireless industries in these countries are unnecessarily duplicating efforts.

The GSMA has confirmed that member operators from a given country can use the GSMA's existing IMEI Database to create a virtual national database. Each operator that connects has its own user profile and part of that profile allows the individual user to select the operators from which it wishes to take data. Therefore, if all Canadian operators are connected to the database and are uploading data, and each operator elects to take data down from the other Canadian operators, a virtual national database is created.

Connecting to the IMEI Database is free of charge, so full national participation avoids the duplication of effort required to build and maintain a separate national database. As well, isolated national databases do not connect into anything else – so handset barring is limited to in-country and devices stolen in that market are free to move and operate in neighbouring markets. Participation in the IMEI Database on the other hand may also reduce the opportunity for exporting stolen phones to other markets.

3. United States

In April 2012, the Federal Communications Commission, major city police chiefs, CTIA and participating wireless companies agreed to the following steps to help protect consumers and their private information on smartphones:

- **By July 1, 2012**: The wireless industry will launch an education campaign for consumers on the safe use of smartphones by using a range of resources, including a public service announcement and online tools such as websites and social media.
- **By October 31, 2012:** US ***GSM*** providers will implement a shared database so that stolen GSM smartphones will not work on any US GSM network.
- **By December 31, 2012**: Smartphone makers will include information on how to secure/lock new smartphones in-box and/or through online "Quick Start" or user guides.
- **By December 31, 2012:** Substantial progress will be made by wireless providers to inform consumers, using communications including email or text messages, about the existence of – and access to – applications that can lock/locate/erase data from smartphones. Providers will also educate consumers on how to access these applications, including those that are easy-to-find and preloaded onto smartphones. This will be completed by April 30, 2013.
- **By April 30, 2013:** Smartphone makers will implement a system to notify/inform users via the new smartphones upon activation or soon after of its capability of being locked and secured from unauthorized access by setting a password.
- **By November 30, 2013:** US providers will create a common database for ***LTE*** smartphones designed to prevent stolen smartphones from being activated or provided service on any LTE network in the US and on appropriate international LTE stolen mobile smartphone databases.[7]

Mobile Theft Deterrence Act

On May 15, 2012, a bill was introduced into the US Congress to “make it unlawful to alter or remove the identification number of a mobile device.” The bill, if passed, would make it illegal, and punishable by up to five years in prison, for anyone to “remove, obliterate, tamper with, or alter” a devices IMEI number, except “the manufacturer of a mobile device or a person who repairs or refurbishes a mobile device unless the manufacturer or person knows that the mobile device or part involved is stolen.”

The bill passed first and second reading and was referred to committee.[8]

AT&T

US provider AT&T announced that it expects to start a program that will keep track of devices that have been reported stolen, making it more difficult for thieves to sell the devices on the black market, beginning the week of July 9, 2012.[9]

[7] http://www.ctia.org/consumer_info/safety/index.cfm/AID/12084
[8] http://www.gpo.gov/fdsys/pkg/BILLS-112s3186is/pdf/BILLS-112s3186is.pdf

AT&T will coordinate its database with other US carriers later this year.

Education Campaign Milestone (July 1, 2012)[10]

In its June 29 quarterly update, the CTIA described the extent to which the industry had met the July 1 milestone of launching an education campaign on the safe use of smartphones. The individual actions of US wireless providers and CTIA are described below:

CTIA

In addition to its broad Public Relations efforts surrounding the launch of the Voluntary Commitment, CTIA has harnessed online and social media to provide valuable information about the industry's Stolen Smartphones initiative to wireless consumers. Specifically, CTIA has:

- Prominently featured on the CTIA website's main homepage (www.ctia.org) detailed information on steps that CTIA and participating wireless companies are taking to deter smartphone thefts.
- Posted 11 blog posts addressing steps to deter smartphone theft and protect user information (including step-by-step "how-to" videos to assist with setting passwords on various smartphones operating systems). These posts have been broadly distributed via social media including Twitter, Facebook, LinkedIn and YouTube.
- Drafted and broadly distributed to newspapers throughout the country a mat release featuring detailed information about steps that consumers can take to help prevent smartphone thefts and safeguard their user information.

CTIA has also engaged an advertising agency and has begun Public Service Announcement concept and production work.

AT&T

AT&T has launched a "vanity" URL at www.att.com/stolenphone to provide detailed information to AT&T wireless customers concerning security tips, reporting a stolen smartphone, and buyer protection options.

AT&T has enhanced its privacy and safety communication and incorporated into new and existing customer communication.

The AT&T sales and support teams have reinforced adding smartphone passwords after activation and provided guidance on downloading apps that help to protect devices and personal information.

Cellcom

Cellcom is on schedule to:

[9] http://bits.blogs.nytimes.com/2012/07/09/att-cellphone-theft/
[10] http://files.ctia.org/pdf/120629_-_FILED_CTIA_Status_Report_on_Industry_Stolen_Phones_Commitment.pdf

- Create a new category on the 'Entertainment & Apps' tab of the Cellcom website and post preloaded and easy-to-use apps to remotely lock/locate/erase data from smartphones. (July 2012).
- Use homepage to share tips on how to avoid unauthorized use of smartphones. (October 2012).
- Use homepage to promote security apps to protect personal information. (November 2012).
- Use auto-generated 'Welcome' email that is sent after new phone activation to encourage use of passwords. (September 2012 and continues).
- E-blast to encourage use of passwords. (October 2012 / January 2013).
- E-blast to encourage use of a mobile security app. (November 2012 / February 2013).
- Launch text messaging campaign to encourage use of passwords. (August 2012 / November 2012).
- Text messaging campaign to promote mobile security apps. (September 2012 / December 2012).
- Target customers who received a smartphone as a holiday gift and share steps to deter cell phone theft and protect personal information. (January 2013).
- Bill stuffer to encourage use of a password and a mobile security app. (January 2013).
- Cellcom newsletter article on how to protect personal information. (November 2012).
- Post statistics and conversation starters on Cellcom's Facebook page. (August 2012 / November 2012).
- Post links on Cellcom's Facebook page to mobile security apps. (August 2012 / November 2012).
- Link to CTIA video(s) on Cellcom's Facebook page. (July 2012).
- Use Twitter to share consumer protection tips. (September/November 2012 / January 2013).
- Share safeguarding tips at close of sale. (Begin in October 2012 and continue).
- Disseminate educational information on passwords and apps to agents. (October 2012).
- Provide Customer Care team with talking points to assist customers with a missing phone. (July 2012).
- Use on-hold messaging to share consumer protection tips.

Nex-Tech Wireless

Nex-Tech Wireless is making plans to develop information on its website to inform consumers about steps to prevent and respond to smartphone theft. The information will become available for online consumers in the coming months.

Sprint-Nextel

Sprint Nextel has created a "vanity" URL webpage at www.sprint.com/stolenphone featuring detailed information on what to do if a smartphone is lost or stolen, encouraging the use of passcodes, and highlighting several mobile security apps that can track, lock and wipe phones. For prepaid users, the company also has created "vanity" URL webpages for its

- Virgin website: http://www.virginmobileusa.com/lost-or-stolen-phone-replacement , and
- Boost website: http://www.boostmobile.com/support/faq/#!/lost-or-stolen-phones

Beginning in June, Sprint Nextel placed bill messages encouraging the use of passcodes and highlighting the availability – and encouraging the use – of applications to track, lock, and wipe smartphones.

Sprint Nextel also launched the Sprint Guardian application in June 2012 designed to help consumers easily set up location-tracking and security apps for Android phones.

Sprint Nextel has also engaged in numerous communications to its customers and internally to highlight the implementation of a blacklist database, information about applications to locate/lock/erase data from smartphones, password protections, and steps to help prevent smartphone theft. These communications include:

- Sprint Press Release on 4-10-12
- Default bill message beginning 6-1-12
- Online Sprint Community blog post 4-18-12
- Sprint Internal Communication 4-12-12
- March 2012 bill insert featured Lookout Security
- March 2012 e-newsletter to base featured Lookout Security

Sprint Nextel also has highlighted the availability of mobile security apps using social media and the company's Sprintzone (a "tile" on the homescreen of Android smartphones).

T-Mobile USA

T-Mobile is on schedule for the July 1, 2012 deadline to begin educational initiatives.

- As a first start, T-Mobile developed and posted a "blog" entry on mobile handset security, referencing T-Mobile resources to obtain additional information.
- Social media tools were used to help propel messaging on the topic to the public.
- Information for customers to help guard against theft and assist when a phone is lost or stolen can be found on T-Mobile.com – including instruction at the "Support" tab on what to do if a phone is lost or stolen and information under "Privacy Resources" which includes tips about password security, protection from identity theft and protection of customer proprietary information.
- T-Mobile's implementation team is currently working on plans to further educate consumers about smartphone theft, protections and preventive measures.

Verizon

In May, Verizon Wireless began its education campaign by launching a consumer-focused web page on Verizonwireless.com that provides customers with information on the prevention of smartphone theft, the importance of using passwords to protect data on smartphones, and what to do if a smartphone is lost or stolen. The site can be accessed at the following link: (http://aboutus.verizonwireless.com/wirelessissues/phonesecurity.html). The site provides direct links to:

- handset manufacturers' app stores where customers can download anti-theft applications.
- register for the company's Wireless Workshops. These classes are offered online and in stores to new and existing Verizon Wireless smartphone customers and are intended to educate its customers on the wide array of powerful features and applications, including security measures.

In July 2012, Verizon Wireless will include information on how to safeguard smartphones and the data on them in the company's monthly newsletter, which is emailed to its customers.

Also as part of its "welcome email" communications program, Verizon Wireless will advise new customers on the availability of passwords to protect the data on their smartphones.

4. United Kingdom

The UK was the first country to introduce broad measures to reduce handset theft, and provides the best example of the potential impact of such solutions.

Table 4: UK operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
T-Mobile (UK) Limited	Pre-2005	18%
Orange PCS Ltd	Pre-2005	18%
VODAFONE Ltd	Pre-2005	25%
Hutchison 3G UK Ltd	Pre-2005	10%
O2 (UK) Limited	Pre-2005	29%
Cable & Wireless UK Ltd.	9-Feb-2009	n/a
Subscribers Connected		100%

All network operators in the UK are currently connected to the GSMA shared IMEI Database, covering all UK wireless subscribers. All major operators were connected prior to December 2004, with the exception of Cable & Wireless UK.

Handset theft reduction solutions have been in place in the UK for a decade, but are constantly being augmented and updated to respond to the ongoing issue of handset theft.

Solutions

IMEI Databases and Blocking

Shared IMEI Database (2002): The UK was the first country in the world to have all mobile phone carriers implementing IMEI blocking and sharing their blocked phone databases (since **2002**).[11] The IMEI blocking initiative included the following time commitments: within 24 hours a reported stolen mobile phone in the UK is blocked by its network provider for use on that network, and within 48 hours 90% are blocked from every network in the country.

National Property Register (2005): *Immobilise.com*, the world's largest free register of possession ownership details, was launched with the support of the cell phone industry, the police and government. Immobilise can be used by members of the public and businesses to register their valued possessions or company assets (including but not limited to cell phones), and exclusive to Immobilise all

[11] http://www.crimeprevention.nsw.gov.au/agdbasev7wr/_assets/cpd/m660001l2/mobile%20phone%20background%20paper.pdf

account holders registered items and ownership details are viewable on the Police national property database the NMPR (www.thenmpr.com). The online checking service is used by all UK Police forces to trace owners of lost and stolen property. In addition Immobilise is checked daily by a huge range of recovery agencies and lost property offices.[12]

Phone Recyclers' Code of Practice (2010): the Telecommunications Fraud Forum, government and police developed a code of practice for phone recyclers to "work closely with police and check the details of every phone they are offered against the national mobile phone register, a database of all phones reported stolen. If the handset has been reported as stolen the company will refuse to buy the phone and details of the phone and the person trying to sell it to them will be passed to police to investigate." It was estimated at the time of enacting the code that 100,000 stolen cell phones were being sold to recyclers every year.[13]

Legislation and Law Enforcement

Reprogramming Act (2002): The Mobile Telephones (Re-Programming) Act 2002 made provisions to prevent the re-programming of mobile telephones. This involves changing the 'unique device identifier' which is the international equipment identification (IMEI) number - i.e. the unique serial number of the phone.

> 1(1) A person commits an offence if:
>
> a. he changes a unique device identifier,
> b. he interferes with the operation of a unique device identifier,
> c. he offers or agrees to change, or interfere with the operation of, a unique device identifier, or
> d. he offers or agrees to arrange for another person to change, or interfere with the operation of, a unique device identifier.
>
> 1(2) A unique device identifier is an electronic equipment identifier which is unique to a mobile wireless communications device.
>
> 1(3) But a person does not commit an offence under this section if:
>
> a. he is the manufacturer of the device, or
> b. he does the act mentioned in subsection (1) with the written consent of the manufacturer of the device.[14]

Mobile Crime Unit (2003): The National Mobile Phone Crime Unit (NMPCU) was officially launched in December 2003.Its main aim is to reduce street crime and the number of mobile phones stolen during these offences by tackling those involved in Mobile Phone criminality; principally the handlers, re-programmers and exporters of stolen mobile phones.[15]

[12] http://www.immobilise.com/about.html
[13] http://www.homeoffice.gov.uk/media-centre/press-releases/code-practice-stolen-mobiles
[14] http://www.met.police.uk/mobilephone/reprogramming.htm
[15] http://www.met.police.uk/mobilephone/

Public Awareness

Out of Your Hands Campaign (2004): The Out of Your Hands campaign and website, launched by the Mobile Industry Crime Action Forum (MICAF) educates young people aged 7 to 16 on the responsible way to own, operate and safeguard your mobile phone (www.outofyourhands.com). The website features downloadable resources specific to three age groups (7-11 year olds, 11-14 year olds, and 14-16 year olds) on how to reduce the potential for cell phone theft.

Crime Reduction Charter (2006): MICAF developed the Mobile Phone Industry Crime Reduction Charter, in which members committed to support:

- Participation in the IMEI blocking initiative.
- The establishment of a specialist marketing group, within MICAF, to develop a program of activity to raise awareness of mobile phone theft.
- The provision of training and information to call centre and retail sales floor staff in respect of crime reduction and false reporting of insurance claims.
- The commissioning of independent research in order to further stakeholders' understanding of the drivers for mobile phone theft.
- The establishment of an agreed testing process between MICAF, NMPCU and The Home Office to measure performance of the UK SEIR (Shared EIR) and commissioning of independent validation of this process.
- The production of an annual report of activity, via MICAF, to review the effectiveness of the industry efforts, the trends in mobile phone theft and the relationship between the two.
- International co-operation in relation to the above objectives wherever appropriate.[16]

Impacts

Theft Reduction

MICAF generally credits IMEI blocking and other initiatives for a 20% drop in cell phone theft in the UK.[17] Media reports on phone theft in the UK, however, are inconsistent, so it is difficult to determine statistical impacts accurately. For instance:

- The **2001** Home Office Research Study provided cell phone theft estimates as high as 700,000 per year.[18]
- A 2006 report cited statistics from **2003** claiming 2,000,000 phones were stolen annually.[19]
- In **2007** the Home Office reported that phone theft was down to 800,000 handsets in England and Wales from 900,000 the previous year.[20]

[16] http://www.micaf.co.uk/uploads/micaf.pdf
[17] http://www.crimeprevention.nsw.gov.au/agdbasev7wr/_assets/cpd/m660001l2/mobile%20phone%20background%20paper.pdf
[18] http://www.martinfrost.ws/htmlfiles/Mobile_phone_theft.pdf
[19] http://www.guardian.co.uk/money/2006/may/16/internetphonesbroadband.phones
[20] http://dalje.com/en-world/security-drive-helps-mobile-phone-theft-fall/44278

- In **2008**, it was reported that mobile phone theft had almost halved since 2003 and was going down year-on-year. July 2008's figures indicated less than 6,000 thefts compared with 11,000 in 2003.[21]
- In **2010**, figures suggested that 228 cell phones were being stolen in the UK every hour, and the government was advocating new innovative ways to tackle phone theft.[22]
- In **2010**, the Express reported that 20,000 phones were reported lost or stolen in the UK every day. That results in **7.3 million** phones lost or stolen for the year.[23]
- In **2012** the BBC reported that approximately 300,000 cell phones were stolen per year in the UK, and that number was rising.[24]
- In advance of the London Olympics, US security firm Venafi predicted that 67,000 handsets would be lost or stolen during the two-week duration of the Games. "50,000 mobile phones are lost or stolen in the London area over any two-week period. During the Olympics, the total population in London is expected to swell by a third, with an extra million people using the tube every day. This, Venafi anticipates, will lead to an additional 17,000 lost or stolen phones, bringing the possible total to 67,000 during the two-week period."[25]

British Crime Survey Results

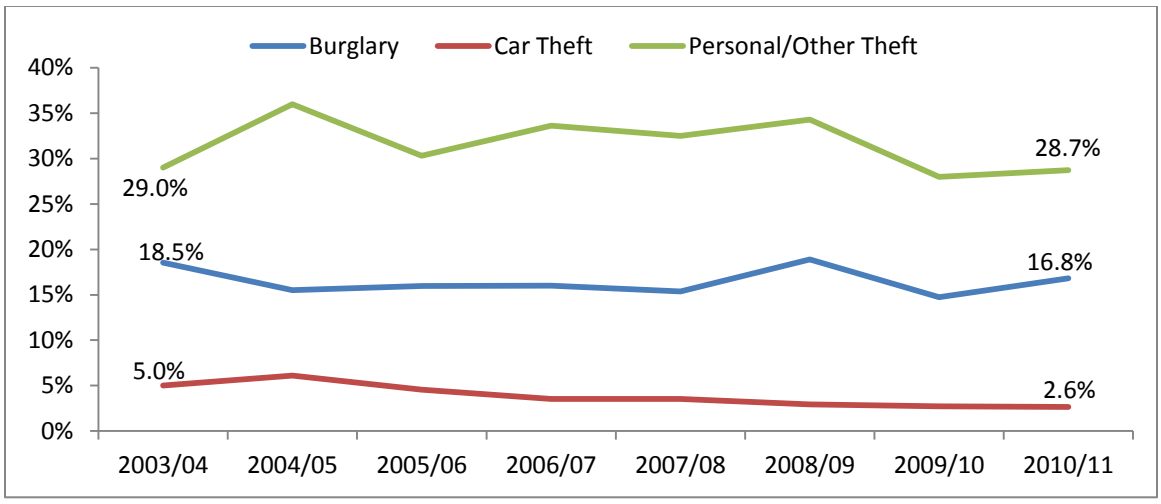
The annual British Crime Survey (known as the Crime Survey for England and Wales since April 2012) provides the most consistent source for annual UK crime statistics. Mobile phone theft appears under the following three categories in the survey:

1. Items stolen in incidents of burglary with entry;
2. Theft from vehicles; and
3. Theft from person and other theft of personal property.

The figure below illustrates the percentage of respondents who reported their mobile phone was stolen as part of an incident in each of the three categories between 2003/04 and 2010/11.

[21] http://www.mobilenewscwp.co.uk/2008/09/mobile-theft-down-but-n96-a-target/
[22] http://news.bbc.co.uk/2/hi/technology/8509299.stm
[23] http://www.express.co.uk/posts/view/218745/Every-day-20-000-lose-their-phone
[24] http://www.bbc.co.uk/newsround/16992837
[25] http://www.venafi.com/67000-phones-likely-to-be-lost-or-stolen-during-london-olympics/

Figure 1: % incidence of mobile phone theft in burglaries, thefts from cars and thefts from people/other[26]



Total handset theft statistics tell a different story. The figure below is based on the application of the percentage of handset thefts to the total number of incidents in each of the three theft categories.

Figure 2: Total handset thefts in burglaries, thefts from cars and thefts from people/other[27]

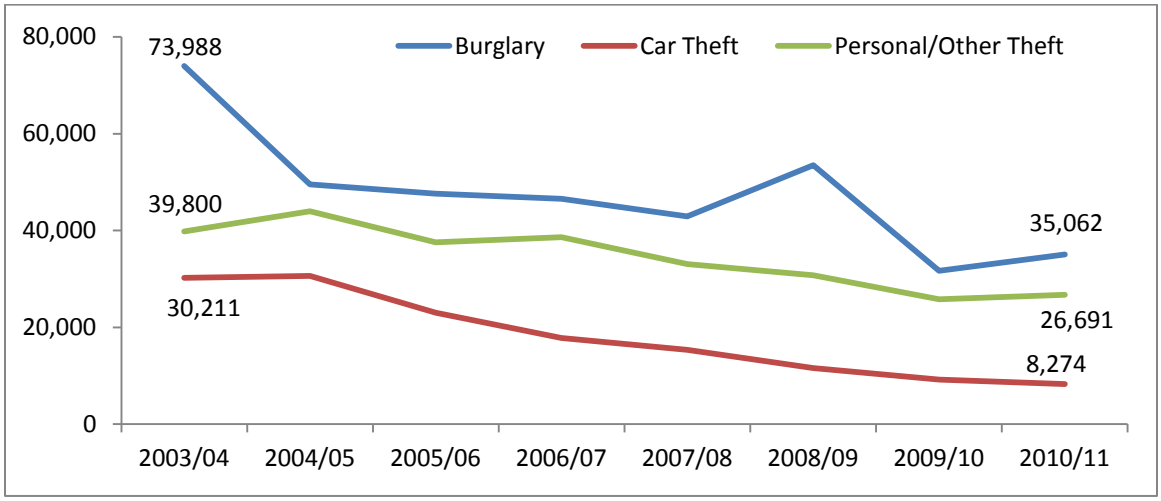
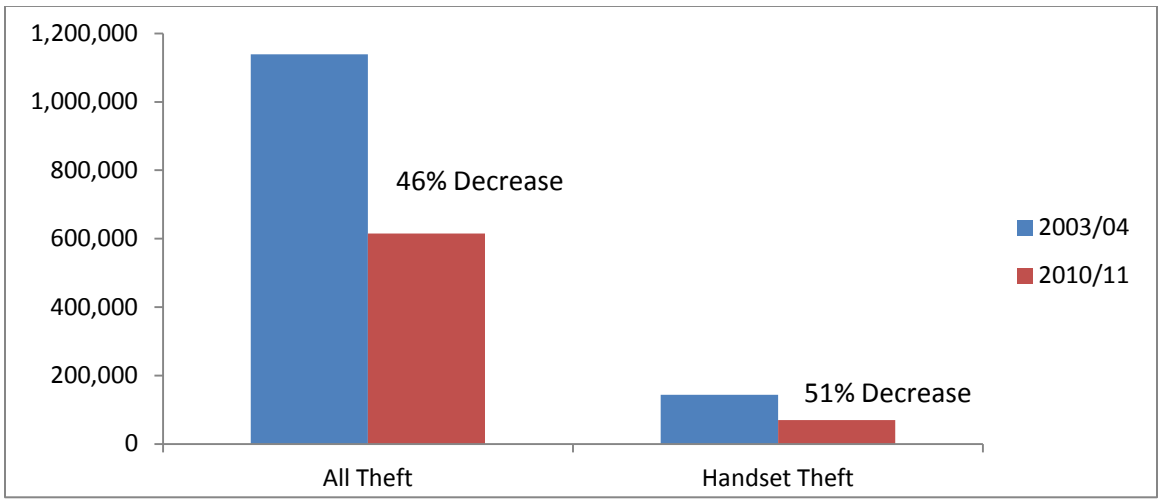


Figure 2 illustrates, according to the crime survey, total handset thefts through burglaries, car thefts and persona/other thefts decreased dramatically over the 7 year period.

Of course, the decline in handset theft is a direct function of the decline in overall thefts as reported by the crime survey. The figure below compares the decline in handset theft with the decline in overall theft between the first and final year of the available data.

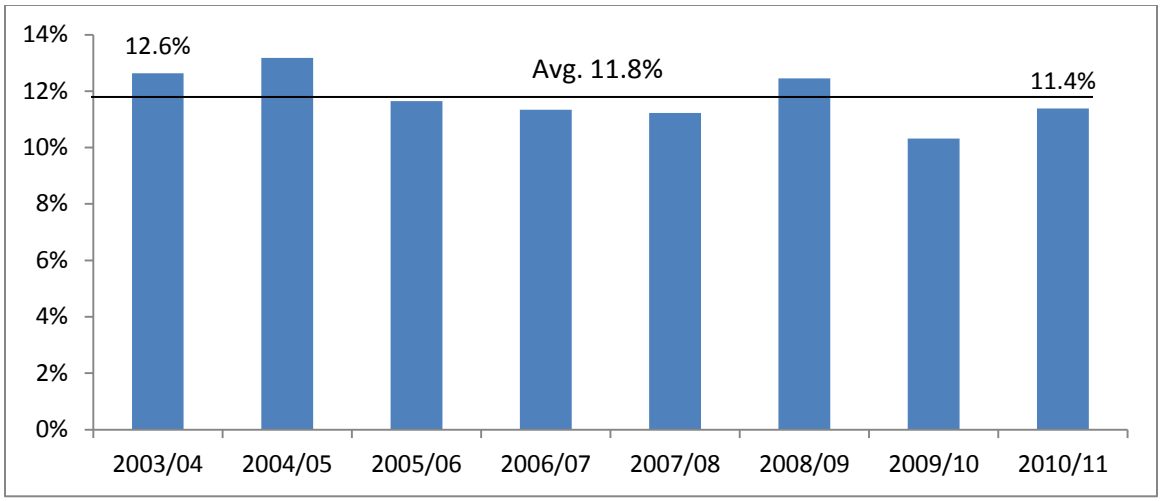
[26] http://www.homeoffice.gov.uk/science-research/research-statistics/crime/crime-statistics/bcs-supplementary-tabs/.
[27] http://homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/hosb1011/?view=Standard&pubID=908823

Figure 3: Decline in theft and handset theft in the UK



Over the seven year period, handset theft declined slightly more than all burglaries, car thefts and personal/other thefts in the UK. Subsequently, the incidence of handset theft as a percentage of total theft also declined slightly during that time and is currently below the 7-year average (as illustrated below).

Figure 4: % incidence of mobile phone theft in burglaries, thefts from cars and thefts from people/other combined[28]



Potential for Abuse

Potential solutions also face the issue of fraudulent claims. A 2010 UK survey on attitudes to mobile phone theft revealed that:

- 18% would be prepared to either damage, lose or take less care of their handset in order to get a new handset; and
- 8% of people say they know someone who has made a fraudulent claim to get a new model.[29]

[28] http://www.homeoffice.gov.uk/science-research/research-statistics/crime/crime-statistics/bcs-supplementary-tabs/.
[29] http://blog.cpp.co.uk/files/uploads/cpp-research/UK_Consumer_Attitudes_to_Mobile_Phone_Theft_2010.pdf

Conclusions

The ongoing implementation of handset theft reduction initiatives in the UK is coincident with the slight decline in handset theft as a percentage of total theft between 2002 and 2011. Major declines in handset theft, however, appear to be a function in overall theft reduction reported by the crime survey. The UK situation additionally demonstrates that measures to combat handset theft can involve broad participation of the industry, law enforcement and the government. Indeed, in spite of ongoing, updated measures (including the addition of a recyclers code of conduct in 2010), recent reports indicate that handset theft is again on the rise.

5. Australia

Australia trails only the UK in terms of implementing a comprehensive handset theft reduction plan. No Australian operators are currently connected to the GSMA's shared IMEI Database, but The Australian Government, Australian Mobile Telecommunications Association (AMTA), and State and Territory police services have implemented a range of initiatives under the 'Mind Your Mobile' campaign to reduce the incidence of loss or theft of mobile phones. The initiatives are described below.

Solutions

IMEI Database and Blocking

Shared IMEI Database (2003): Australia's three national network providers – Optus, Vodafone and Telstra – launched an Industry-wide handset blocking (using the IMEI number) initiative. The three carriers agreed to send a list of lost, stolen or found mobile phones to each other "every day or so" so the reported handsets could be blocked or unblocked on all networks within 36 hours. [30]

Online IMEI Status Check: the Mind Your Mobile website allows Australian's to check the status of an IMEI in real-time to determine if a second-hand handset has been reported as lost or stole (https://prod.eie.net.au/portal/template/MYMIMEIInquiry.vm).

Legislation and Law Enforcement

IMEI Modification Legislation (2004): The Australian government added "modification of the International Mobile Equipment Identity (IMEI) number of mobile phones" to the list of offences in its criminal code in 2004. [31] Altering an IMEI is punishable by up to two years in prison. [32]

Public Awareness

Mind Your Mobile: A public awareness campaign was set up through www.mindyourmobile.com to increase consumer awareness of the steps users can take to prevent theft. Of note, roughly 50% of cell phones stolen in Australia are taken from cars, so the public awareness focused partially on not leaving phones in areas where they could be targeted.

---

[30] http://www.crimeprevention.nsw.gov.au/agdbasev7wr/_assets/cpd/m660001l2/mobile%20phone%20background%20paper.pdf

[31] http://www.austlii.edu.au/au/legis/cth/bill_em/claoaomb2004712/memo1.html

[32] http://www.crimeprevention.nsw.gov.au/agdbasev7wr/_assets/cpd/m660001l2/mobile%20phone%20background%20paper.pdf

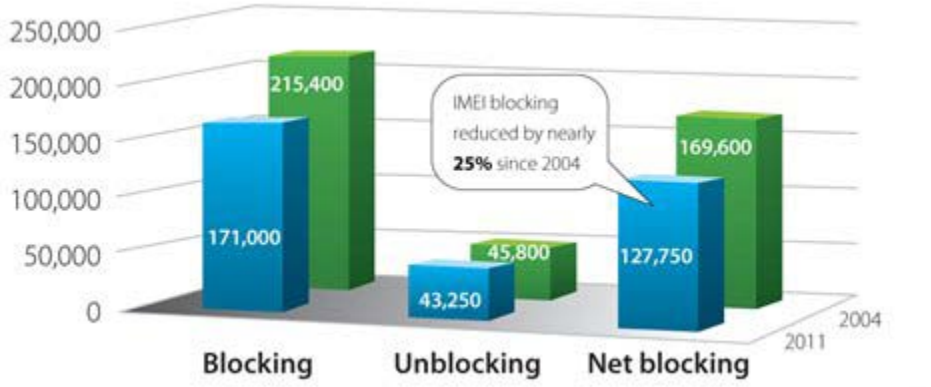
Impact

Cost

At the time of launching the stolen phone blocking initiative (2003), the AMTA reported that the industry had spent $7 million on technology to block IMEI numbers.[33]

Theft Reduction

In the first four years of the Mind Your Mobile program, AMTA reported a 30% reduction in the number of handsets blocked annually across Australia. By 2011, the number had stabilized at roughly 170,000 handsets blocked per year, with 43,000 of those eventually being unblocked after being found or returned – a 25% reduction in net blocks over the seven year period. [34] The figures below are indicative of the number of stolen and lost handsets in Australia, but are limited only to those incidences which were reported to network operators.



The territory of New South Wales (which includes the city of Sydney) keeps detailed statistics on phone theft. The NSW bureau of crime statistics reported that cell phone theft increased dramatically between 1999 and 2000, rising from 24,274 incidents to 39,891 incidents. Between 2008 and 2011, cell phone theft in the territory was relatively level, averaging 22,051 incidents per year.

Cell phone theft figures from the available years in New South Wales are provided in the table below.

Table 5: Cell phone theft, New South Wales, Australia (reported incidents per year; available years)[35]

	1999	2000	2008	2009	2010
New South Wales	24,274	39,891	22,627	21,236	22,289

IMEI Reprogramming/Phone Reselling

Although legislation was passed to make tampering with an IMEI illegal in Australia, phone thieves and their customers are increasingly breaking that law to reactivate stolen phones. In 2010 the AMTA

[33] http://www.amta.org.au/pages/amta/The.Mobile.Phone.Industry.Statement
[34] http://www.amta.org.au/articles/Figures.show.mobile.phone.thieves.get.the.message.about.IMEI.blocking
[35] http://www.crimeprevention.nsw.gov.au/agdbasev7wr/_assets/cpd/m660001l2/mobile%20phone%20background%20paper.pdf

president noted that the industry had witnessed a significant increase in the number of duplicate IMEI numbers in Australia due to re-programming of stolen phones.[36]

Also, while law enforcement participation is a critical component handset theft reduction, New South Wales police confirmed in 2010 that it was selling between 400 and 500 handsets per year at police auctions without checking the status of the IMEI numbers.[37]

Conclusions

The handset theft data from Australia clearly shows a decline in handset theft – and the number of phones reported lost/stolen – following the launch of the Mind Your Mobile campaign and the supporting legislation. As stated by the figures on cell phones reported stolen or lost, and the theft figures from New South Wales, the overall initial decline was around 25% and cell phone theft has leveled off. Based on the data from Australia's IMEI database, about 125,000 stolen/lost phones are unrecovered each year.

6. Europe

France

Table 6: French operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Bouygues Telecom	Pre-2005	18%
Orange France	Pre-2005	47%
SFR - CEGETEL	Pre-2005	35%
Subscribers Connected		100%

All major French network operators are connected to the GSMA IMEI Database, covering 100% of French subscribers. France has also been proactive in implementing national theft reduction measures, described below.

Solutions

IMEI Database and Blocking

Shared IMEI Database (2003): French network operators set up a shared database of phones reported lost or stolen in 2003.[38]

IMEI Blocking Upgrade (2011): An improved process for blocking phones reported lost or stolen was introduced in France by the Federation Francaise des Telecoms on March 15, 2011.[39]

[36] http://www.theaustralian.com.au/australian-it/mobile-buyers-beware-cops/story-e6frgakx-1225855710892
[37] http://www.theaustralian.com.au/australian-it/mobile-buyers-beware-cops/story-e6frgakx-1225855710892
[38] http://www.cellular-news.com/story/37901.php
[39] http://www.fftelecoms.org/faq/quelles-sont-les-demarches-que-le-client-doit-effectuer-pour-interdire-lutilisation-frauduleuse

Legislation and Law Enforcement

Phone Blocking Law (2011): While French network operators had been sharing a database of lost/stolen phones since 2003, a law requiring stolen phones to be blocked was not introduced until 2011.[40][41]

Anti-tampering law: Reprogramming an IMEI in France is an offence punishable by up to two years in prison and a €37,500 fine.[42]

Public Awareness

Radio Campaign (2008): The French mobile operator association AFOM ran a radio advertising campaign backed by Nokia, Samsung and Sagem on the risks of mobile phone thefts, advising users to note the international mobile equipment identity (IMEI) number of their handsets and to provide it to their operator if their phone is stolen.[43]

Mobile volé, mobile bloqué (2011): the public awareness website (http://mobilevole-mobilebloque.fr/) was launched in October 2011 to educate French mobile users about IMEI blocking and handset security. The site allows visitors to enter their IMEI number and email address, mailing their IMEI number back to them so they will be able to report it to their provider if their phone is stolen or lost.

Impact

Theft Reduction

Stolen phone blocking measures and updated phone blocking measures in France both returned positive results. For instance:

- The French National Police Administration reported that cell phone thefts fell from 174,250 in 2007 to 156,500 in **2008**, a 10.19% decline.
- French newspaper *Le Monde* reported that mobile theft in France dropped 20% between April 2011 and April **2012**, following the introduction of the improved process for blocking stolen phones.[44]

IMEI Reprogramming

In 2012, the Paris police department announced that it had discovered the use of software called Z3X, which has apparently been found in 50 mobile phone shops in eastern Paris. Z3X is a Ukrainian-made tool that offers what appears to be a specific way to reset IMEI numbers on various specific phones, including models of Samsung, LG, NEC and other phones. The group has listed resellers scattered across the United States, Europe, Russia, Ukraine, and Libya.[45]

Conclusions

Similar to the UK and Australia, France reports 10-20% declines in cell phone theft following the implementation of theft reduction initiatives.

---

[40] http://www.mobiledia.com/news/79377.html
[41] http://arstechnica.com/tech-policy/2012/06/police-mobile-software-hack-defeating-anti-theft-measure/
[42] http://arstechnica.com/tech-policy/2012/06/police-mobile-software-hack-defeating-anti-theft-measure/
[43] https://www.neurope.eu/article/mobile-phone-thefts-fall-charts
[44] http://arstechnica.com/tech-policy/2012/06/police-mobile-software-hack-defeating-anti-theft-measure/
[45] http://arstechnica.com/tech-policy/2012/06/police-mobile-software-hack-defeating-anti-theft-measure/

Netherlands

No Dutch network operator is connected to the GSMA's IMEI Database. However, the Netherlands was among the first European countries to attempt to curb the issue of mobile phone theft.

Solutions

IMEI Blocking

Vodafone Bans Stolen Phones (2005): Vodafone announced in late 2004 that it would become the first mobile operator in the Netherlands to be able to permanently ban stolen phones of its customers on Vodafone's mobile network.[46] At the time, Vodafone was blocking stolen phones through its Equipment Identity Register in 11 countries. As is clear in Table 1, Vodafone is the most active network operator in terms of blocking stolen phones; in Egypt, Germany, Malta, Portugal and Spain, Vodafone is the only operator connected to the IMEI Database.

Law Enforcement

Text Bombing (2001): Amsterdam police began deterring cell phone theft by sending SMS messages to stolen phones. When a victim reported a theft, police sent an SMS message every three to five minutes to the stolen phone that said: "You are in possession of a stolen cell phone. Did you know that stealing a cell phone is a crime punishable by imprisonment? Using a stolen cell phone is too, and you are risking a prison term of one year."[47]

Impact

Theft Reduction

Early reports indicated that the text bombing initiative reduced cell phone theft in Amsterdam by approximately 50% within a year, and text bombing was eventually adopted by police in Rotterdam as well.[48]

Overall, cell phone theft remains an issue in the Netherlands, for instance:

- In **2004** it was reported that 240,000 cell phones were stolen per year in the country.[49]
- In **2011**, Vodafone dealt with 55,000 reports of lost or stolen mobile phones in the Netherlands.[50]
- A **2011** study by the National Academy for Media and Society revealed that one in five people in the Netherlands had either lost their phone or had it stolen. That number increase to one-in-three for people in their teens and twenties.

[46] http://www.telecompaper.com/news/vodafone-netherlands-to-ban-stolen-mobile-phones
[47] http://www.time.com/time/magazine/article/0,9171,214207,00.html
[48] http://www.time.com/time/magazine/article/0,9171,214207,00.html
[49] http://www.telecompaper.com/news/vodafone-netherlands-to-ban-stolen-mobile-phones
[50] http://www.dutchnews.nl/news/archives/2012/05/one_in_five_mobile_phones_lost.php

Roadblocks

The text bombing strategy raised questions about the legalities of police obtaining cell phone numbers without a warrant. Also, service providers were expected to bear the cost of the texts and subsequently some declined to participate in the initiative.[51]

Italy

Table 7: Italian operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodafone Omnitel N.V.	Pre-2005	32%
Telecom Italia Mobile	Pre-2005	35%
Wind Telecomunicazioni SpA	Pre-2005	23%
H3G	Pre-2005	10%
Subscribers Connected		100%

All major network operators in Italy, covering all subscribers, were connected to the GSMA IMEI Database prior to December 2004.

Solutions

Italy's four mobile phone companies agreed to introduce a joint register of stolen phones in early 2002. At the time it was reported that phone theft was not a major issue in Italy.[52]

There is no additional information available on the status or impacts of the joint phone database in Italy.

Germany

Table 8: German operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodafone D2 GmbH	9-Feb-2005	33%
Subscribers Connected		33%

Vodafone is the only network operator in Germany connected to the IMEI Database.[53] There are no additional handset theft prevention measures in place in Germany.

Austria

No Austrian network operators are connected to the IMEI Database. It was reported in 2009 that 28,000 mobile phones were stolen in Austria every year.

[51] http://www.time.com/time/magazine/article/0,9171,214207,00.html
[52] http://www.computerweekly.com/news/2240043810/Italian-mobile-operators-unite-against-phone-theft
[53] http://www.telecompaper.com/news/vodafone-germany-introduces-security-service-for-lost-or-stolen-handsets

Ireland

Table 9: Irish operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Meteor Mobile Telecommunications Limited	Pre-2005	n/a
O2 Ireland	Pre-2005	n/a
Hutchison 3G Ireland limited	1-Aug-2005	n/a
Vodafone Ireland Ltd	9-Nov-2005	n/a
Subscribers Connected		100%

Sweden

Table 10: Swedish operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Telenor Sverige AB	Pre-2005	16%
TeliaSonera Mobile Networks AB	Pre-2005	46%
Tele 2 AB	1-Aug-2005	27%
Hi3G Access AB	28-Nov-2007	10%
Subscribers Connected		100%

Denmark

Table 11: Danish operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
TDC Mobil A/S	Pre-2005	44%
Telia A/S Denmark	Pre-2005	18%
Sonofon	18-Jan-2010	25%
Subscribers Connected		86%

Belgium

Table 12: Belgian operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Belgacom Mobile	Pre-2005	41%
Mobistar S.A.	Pre-2005	28%
BASE NV/SA	Pre-2005	26%

Subscribers Connected	100%[54]

Czech Republic

Table 13: Czech operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Telefonica O2 Czech Republic, a.s.	22-Jun-2005	36%
Subscribers Connected		36%

Finland

Table 14: Finish operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
DNA Oy	Pre-2005	24%
Sonera Mobile Networks Limited		35%
Subscribers Connected		59%

Norway

Table 15: Norwegian operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Telenor Mobile	Pre-2005	34%
NetCom AS	Pre-2005	28%
Subscribers Connected		82%

Spain

Table 16: Spanish operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodafone Espana S.A.	Pre-2005	30%
Subscribers Connected		30%

Portugal

Table 17: Portuguese operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodafone Portugal	Pre-2005	36%

[54] Source: GSMA.

Subscribers Connected	36%

7. CITEL[55] & Latin America

On May 30, 2012, CITEL (Comisión Interamericana de Telecomunicaciones Inter-American Telecommunication Commission) adopted its Final Resolution on Handset Theft. In prefacing the resolution, the delegation of Columbia noted that in 2009, 2.1 million terminal devices were stolen in Columbia, a figure that, according to police records, rose to 3 million in 2010.

As such, the Administration of Colombia invited Member States to implement the following actions to combat the theft of these devices:

1. Adopt, strengthen, or complement the measures needed, each within its sphere of competence, to minimize as much as possible the theft of mobile terminal devices and their activation and marketing at the regional level.
2. Encourage their national mobile service operators that do not yet have them to consider implementing negative lists (black-lists) database that have a registry of the IMEIs or manufacturer's electronic serial numbers of mobile terminal devices reported stolen or lost nationally .
3. Use, among other existing alternatives, platforms such as the GSMA IMEI DB, in view of the benefits it can afford countries, their regulatory entities, and operators in terms of cost, operating infrastructure, and experience in the exchange of IMEIs of devices reported stolen or lost.
4. Invite the CDMA Development Group (CDG) to present to CITEL, insofar as possible, options for the exchange of blacklists for CDMA terminal devices similar to those presented by GSMA for GSM terminal devices.
5. Take relevant actions in accordance with their regulatory framework to exchange at the international level blacklists of stolen or lost mobile terminal devices through the signature of bilateral or multilateral agreements.
6. Consider including in their regulatory frameworks the prohibition of the activation and use of the IMEIs or manufacturer's electronic serial number of devices reported stolen, lost, or of unlawful origin in regional or international databases.
7. Collaborate, in coordination with the industry, in defining and implementing technical-operational solution options facilitating the suspension of all services and applications of mobile terminal devices that have been reported stolen and/or lost in national or international databases.
8. Conduct campaigns to raise public awareness of the importance of reporting the theft and loss of their mobile terminal devices.
9. Present to PCC.I at its next meeting informational documents containing the results of actions carried out and steps taken with the aim of evaluating and discussing the complementary actions implemented in this area.

[55] http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf

10. Conduct information and awareness campaigns against the acquisition of mobile terminal devices of unlawful origin.

GSMA Latin America

In July 2012, the GSMA Latin America announced that all of the major network operators in Latin America had committed to start sharing stolen handset information via the GSMA's IMEI Database. The initiative is expected to be fully implemented by March 2013, and will cover more than 500 million phones in Latin America.[56]

The table below lists the network operators that have committed to the initiative, and the Latin American countries in which they operate.

Table 18: Latin American operators participating in stolen handset database

Operator	Countries
America Movil	Mexico, Brazil, Columbia, Argentina, Paraguay, Uruguay, Puerto Rico, Guatemala, Nicaragua, El Salvador, Honduras, Panama, Ecuador, Peru, Dominican Republic, Jamaica, Chile, Costa Rica
Antel	Uruguay
Cable & Wireless Panama	Panama
Corporacion Digitel	Venezuela
Entel Bolivia	Boliva
Entel Chile	Chile
ICE	Costa Rica
Tigo Columbia	Columbia
Nextel/NII Holdings	Argentina, Brazil, Chile, Mexico, Peru
Nuevatel PCS Bolivia	Bolivia
Orange Dominican Republic	Dominican Republic
Telecom Italia	Brazil
Telefonica	Argentina, Chile, Columbia, Costa Rica, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Peru, Uruguay, Venezuela

Costa Rica

Table 19: Costa Rican operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
ICE Costa Rica	18-Jul-2005	n/a
CLARO CR TELECOMUNICACIONES	7-Feb-2012	n/a
Telefonica de Costa Rica TC	18-May-2012	n/a
Subscribers Connected		100%

[56] http://www.cellular-news.com/story/55429.php?source=rss

As of May 2012 all three network operators in Costa Rica were connected to the IMEI Database, making Costa Rica the first Latin American to do so.

Chile

Table 20: Chilean operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Movistar Chile	8-Nov-2005	39%
Subscribers Connected		39%

Venezuela

Table 21: Venezuelan operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Corporacion Digitel C.A.	18-Oct-2011	n/a
Subscribers Connected		23%

8. Africa

To date there are no comprehensive pan-African initiatives to attempt to reduce cell phone theft. However, a number of African countries have taken steps to deter handset theft, including connecting to the IMEI Database, as described below.

South Africa

Table 22: South African operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodacom Group Pvt Ltd.	Pre-2005	50%
Subscribers Connected		50%

Vodacom is the only network operator in South Africa connected to the IMEI Database. However, all South African operators have been cooperating on reducing cell phone theft for the past seven years.

Solutions

IMEI Database and Blocking

Shared Blacklist (2005): South Africa's three service providers – Cell C, MTN and Vodacom – signed an agreement, along with the non-profit group Business Against Crime and the South African Police Service, to maintain and share blacklists of IMEI numbers for phones reported lost or stolen.[57]

[57] http://www.cellular-news.com/story/12585.php

Legislation and Law Enforcement

RICA Legislation (2009): In July 2009, the South African government passed what is known as the RICA (Regulation of Interception of Communication Act) which made it compulsory for everyone in South Africa (including businesses) to register all new and existing SIM card numbers by June 2011.[58] Operators who failed to comply with the deadline could have been fined up to 2 million Rand, and be forced to disconnect non-compliant customers. The RICA legislation also made it compulsory to report the loss, theft or destruction of a cell phone or SIM card, making it an offence not to do so. [59]

Impact

Theft Reduction

There are no available statistics on the impacts of the various theft reduction measures in place in South Africa. However, the South African Police Service reported in 2009 (five years after the shared blacklist was put in place) that cell phones were by far the most reported stolen or lost item in South Africa, with more than 15,000 cell phones being stolen every month and more than 1 million stolen cell phones in circulation.[60]

Egypt

Table 23: Egyptian operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Vodafone Egypt Telecommunications S.A.E	Pre-2005	37%
Subscribers Connected		37%

Kenya

Table 24: Kenyan operators connected to the GSMA IMEI Database, date of connection, and national subscriber share

Operator	Date of Connection	Subscriber Share
Celtel Kenya Ltd.	Pre-2005	n/a
Subscribers Connected		16%

9. Asia-Pacific

Although not as comprehensive as Australia, a number of countries in the Asia-Pacific region have explored, or are currently exploring, measures to deter handset theft.

[58] http://www.geotab.co.za/index.php?option=com_content&view=article&id=27&Itemid=29
[59] http://www.bac.co.za/Art/Newsletters/BACSA%20NL%20June%202011.pdf
[60] http://www.link2media.co.za/index.php?option=com_content&task=view&id=6421&Itemid=15

India

India has considered and examined the possibility and feasibility of various theft deterring measures over the past decade. For instance:

- The Telecom Regulatory Authority of India (TRAI) first examined IMEI blocking in **2004**. However, at that time, a number of service providers did not have the capability to track/block the handset in their network.[61]
- In **2008**, TRAI ordered that network operators retain IMEI logs, and that handsets without a valid serial number be blocked from the individual networks.[62]
- In **2010**, TRAI launched a new consultation on industry-wide IMEI blocking.
- As of November **2011**, it was anticipated that TRAI would announce recommendations on IMEI blocking (no recommendations have been released to date).[63]

Malaysia

It was reported in June 2012 that a third-party company had been set up to manage an independent clearing house that will "blacklist" stolen handsets and bar them for being used again. The plan involved operators paying RM 1.5 (about 32 cents) per IMEI, but the industry responded that they could establish and manage a blacklist at a lower cost. [64]

New Zealand

Two of the three major network operators in New Zealand have some handset theft measures in place. Vodafone disables stolen phones' SIM cards and blocks the handset from its network after receiving a report of a theft. And Telecom bars stolen phones from any outgoing activity and allocates customers a password to reactivate the phone if it is recovered.

Neither system can stop phones being sold on or used again on another network. As of April 2012, the operators were not working on any joint initiatives.[65]

[61] http://www.cellular-news.com/story/46248.php
[62] http://www.cellular-news.com/story/46248.php
[63] http://www.hindustantimes.com/News-Feed/SectorsInfotech/Trai-recommendations-on-blocking-lost-stolen-mobiles-by-Dec/Article1-771600.aspx
[64] http://thestar.com.my/news/story.asp?file=/2012/6/25/business/11518847&sec
[65] http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10799786