

# Progress and Prospects in the Prevention of Mobile Phone Theft

JEN MAILLEY,\* SHAUN WHITEHEAD† and GRAHAM FARRELL‡

Mobile phone ownership continues to be a driver of theft and robbery in the UK. Several years of news headlines such as “Mobile Phones and iPods fuel rise in Muggings” ((2006) *Independent*, February 27,) suggest that the problem may be getting worse rather than better. Whether this is true probably depends on what is measured. It is likely that total crimes have remained stable or increased at the same time as risk-per-phone-owner has decreased. The latest Ofcom figures show that in 2005-6, the UK’s mobile phone subscriptions exceeded the population for the first time, having doubled in the last five or six years. The country being awash with mobile phones, stealing them is like shooting the proverbial fish in a barrel. We argue below that progress has been made in tackling mobile phone theft and that this is not incompatible with an increase in the problem, which would have been even greater without the measures taken to date. There may be a case for cautious optimism – but only if efforts to prevent mobile phone theft continue to be at least as persistent, innovative and adaptable as the thieves themselves to the point where the problem is stabilized and diminishes thereafter. Government, police and the mobile industry, working together, have a technological and geo-political advantage over offenders that, with a lot of skill and dogged determination, could yield absolute crime reductions in the future. What follows reviews some of the progress to date in tackling mobile phone theft and suggests this should form a platform for an expanded crime prevention effort.

## Progress

The landmark research study in this field was “Mobile Phone Theft” by Pat Mayhew and Victoria Harrington (2001, Home Office Research Study 235). It was the first report to produce methodologically justifiable estimates of the extent of the national problem. Among other things, the report suggested there were 710,000 mobile phone thefts in the UK in 2000, that the victims were disproportionately young people, and that mobile phones were a target in a third of all robberies. The report continues to be influential because its thoroughness is unmatched in the UK and because few governments outside the UK have attempted comprehensive studies. While we in the UK may think we

are still clutching at evidential straws, other countries are generally less informed about the problem (and in some cases, images of ostriches and sand spring to mind). The rest of this section outlines UK progress in three key areas. Legislation and law enforcement are followed by a brief review of the collaborative effort between Government and the mobile phone industry.

Legislatively, the Mobile Telephones (Reprogramming) Act 2002 is the principal reference point. It outlawed the changing of handset identities, that is, the changing of the unique security number (the International Mobile Equipment Identity or IMEI) that is programmed into each handset. An amendment as part of the Violent Crimes Bill (pending at the time of writing) will outlaw offers or agreements to alter IMEIs. The significance of the legislation becomes clearer when blacklisting and reprogramming are described below.

Police throughout the UK have become increasingly aware of issues relating to mobile phone theft. The Robbery Reduction Programme of 2002 and the Street Crime Initiative of 2002 to 2005 were high profile policing attempts to tackle such theft. The more recent development has been the work of NMPCU (the National Mobile Phone Crime Unit) since its inception in December 2003. Situated in London, NMPCU is, to our knowledge, the only national-level police unit, in any country, dedicated to tackling mobile phone crime. It undertakes street-level stings and other operational activities, and rapidly became a source of expertise.

The focus in what follows is on the collaborative efforts of the mobile phone industry. Manufacturers, networks, and industry bodies have worked together and with Government and the police, to develop new policies and crime prevention measures. In a highly competitive industry, this collaboration should not be taken for granted and any progress to date is the product of much time and effort on the part of those involved. While corporate social responsibility is, of course, a laudable and marketable aim, our meetings and conversations with a range of those involved in the industry have repeatedly left us impressed with the level of genuine desire to see crime reduced and to continue to respond to its changing profile. Having said this, the goal of business quite rightly is profit rather than the protection of the consumer against crime, and so there remains an appropriate watchdog role for Government, police, and policy-makers. This in turn, could generate market forces that make security a marketable part of the industry as it has increasingly become in relation to cars and homes.

The Mobile Industry Crime Action Forum (MICAF),

\* Research Associate, Midlands Centre for Criminology and Criminal Justice, Loughborough University.

† Engineer and Research Associate in the Department of Design and Technology at Loughborough University.

‡ Professor of Criminology, Director, Midlands Centre for Criminology and Criminal Justice, Loughborough University.

chaired by Jack Wraith MBE, emerged in 2000 from the former Crime Action Group. It includes representatives from mobile network operators, mobile phone manufacturers and major retail outlets. Since networks and manufacturers are competitors, MICAFA was set up to coordinate UK intra-industry activity in an area wherein they all agreed collaboration is necessary and fruitful: crime reduction. The other major industry player is the international GSM Association (GSMA), based in Dublin, an umbrella organization for network operators. The GSMA hosts the international IMEI database, the Central Equipment Identity Register (CEIR), which has the potential to drive international collaborative efforts in the future, as detailed below. The next paragraphs in this section briefly describe the blacklisting and reprogramming of mobile phone handsets to set the scene to assess progress and prospects.

#### *Handset Blacklisting*

Each mobile handset is programmed with a unique IMEI (International Mobile Equipment Identity) number. The IMEI is separate from the identity of the SIM card (the small card which typically sits under the battery in the handset). The SIM card identity is linked to the phone number and to call-billing. On each network, any call that is made is linked both to the handset IMEI identity and to the SIM card identity. A handset's IMEI can be checked by typing \*#06# on the keypad. The IMEI is used by the networks to blacklist stolen handsets. The database which allows network operators to share the identities of blacklisted handsets, the CEIR, was set up in 2002 following pressure from Government on some operators. Operators differ slightly in the way they use blacklisting. Some blacklisted handsets can still receive texts on some networks, for example, while others cannot. This is an imperfect state of affairs, the ideal being for all providers to remove all functionality from blacklisted handsets.

The UK's main network operators (T-mobile, Vodafone, O2, Orange, 3) have been working hard to implement the blacklisting of stolen handsets. It is not as simple as it sounds. It takes software programming, some training of call operators and coordination of blacklisting data. While practices vary by network, at the Vodafone call centre in Oxfordshire a dedicated team of four staff monitor the blacklisting, acting as quality controllers of the work done by the "front line" call handlers. This is a considerable task since thousands of handsets are reported stolen or lost every month. There may yet be kinks to be ironed out in the process but the industry has taken the lead via a report commissioned by MICAFA. The study, carried out by System Concepts, employed a "secret shopper" methodology to purchase handsets, report them stolen, then measure if and how quickly they were blacklisted. It found that all networks failed to blacklist some proportion of the "stolen" handsets. An unpublished small-scale study by Roni Garcia at NMPCU looked at whether phones reported as stolen to the police were blacklisted. Preliminary findings suggest 30 to 40 per cent were not. These somewhat troubling results are being used by networks to hone current policies and practices. The system appears to run smoothly in blacklisting stolen SIM-cards. We would anticipate similar success with respect to handset blacklisting in the near future.

#### *Reprogramming*

If a stolen handset is blacklisted it is useless in the UK, and so, in theory, there is little point in stealing it. To overcome this, some offenders change (reprogramme or "flash") the IMEI number to alter the identity of the handset, thereby assigning it a fake identity, usually a duplicate of the IMEI from a licit handset. The reprogrammed handset will then work and becomes difficult to trace and reblacklist. A little specialist skill and equipment are needed to undertake reprogramming, and these skills seemed to spread fairly rapidly to handset repair shops and other sources. Hence the Home Office introduced the 2002 Mobile Telephones (Reprogramming) Act to outlaw the procedure. Simply put, reprogramming encourages further theft and robbery, and promotes spin-off criminal activities (at a minimum, the resale and continued use of a stolen handset).

Handset manufacturers have ratcheted-up the effort required to reprogramme a handset by increasing handset hardware and software security. The possibilities include improved software encryption, dispersing the IMEI on various chips in the handset to make it harder to locate and change, and making more of the IMEI hardware-based rather than software based (since it is software that is reprogrammed). The industry has produced and disseminated "nine principles" to promote handset integrity and developed a reporting system to identify known breaches.

There is now an additional market incentive to improve handset integrity and to remove illegal IMEI duplicates from the network systems. There is no standard format for how content (video, images) will be displayed on a handset, so in order to know how to format the content for one person's device, the network operator needs to know the make and model of that particular phone (since screen sizes and capabilities vary). The easiest way to do this is to look at the handset IMEI to determine the make and model. The model label will be incorrect for reprogrammed handsets. Hence operators may now have some vested and growing financial interest in limiting illegal-duplicate IMEIs.

### **Adaptations in the Crime Market**

If blacklisting were fully implemented and reprogramming halted, there would not be much of a market for stolen phones in the UK, and no financial reward to the thief. In practice, the crime market has adapted. To be optimistic, such adaptations may well be responses to crime prevention interventions, and thus capable of interpretation as partial indicators of the impact of crime prevention measures.

The first possible adaptation by offenders is a decline in reprogramming. Like many of the issues described here, it appears difficult to quantify the extent of this change. If real, this adaptation could plausibly be the result of the impact of the measures described above to tackle reprogramming, including police sting operations against repair shops and other outlets. Due to rapid turnover and replacements, new handsets penetrate the market quickly, so improved handset IMEI security will kick in correspondingly quickly (unlike, say, when steering wheel locks were made compulsory on new cars and they took many years to become commonplace because the stock of cars is replaced more slowly).

A second key adaptation by offenders is that handsets stolen in the UK appear to be increasingly shipped for re-

sale overseas. In addition to handset seizures at customs, we know of only one small-scale study, conducted by Kevin England of O2 in collaboration with NMPCU, which showed that handsets stolen in the UK were turning up in dozens of countries around the world. Again there is a dire need for further quantification. If handsets are being increasingly shipped overseas this might be a further partial indicator of the impact of crime prevention measures in the UK. Blacklisted handsets cannot be used on UK networks but can still be used elsewhere. We view this as a qualified success for crime control because it takes more time, effort, money, resources and connections for criminals to ship handsets overseas for resale. If other things remained equal, illicit profit margins would be down. Another indicator of successful adaptation/displacement is evidenced on eBay, where stolen “blocked” handsets are now advertised with the proviso that they cannot be used in the UK. The information is conveyed by the seemingly innocuous statement that the seller is “only shipping to non-UK countries”. The Home Office is reputedly approaching eBay to discourage the auction site from further becoming an e-fencer of stolen goods and facilitator of international trafficking.

One possibility to limit the international traffic currently under consideration lies in restricting handsets to use on UK networks. Hence, for example, a South African SIM-card would not operate in a UK handset. The issues here are the possibility of restrictive business practices plus the possibility that consumers travelling overseas would incur higher roaming charges if obliged to use a UK network. Such issues remain to be resolved.

Other factors influence the dynamics of mobile phone theft. For many products such as video cassette recorders, once the UK market was saturated (that is, everyone who wanted a VCR had one), there was little or no resale market for stolen VCRs, particularly since the retail price of the technology had also plummeted over time. Mobile phones are different for two reasons. First, many people change and upgrade their handset regularly. Markets with rapid turnover (at the most extreme, think of the market for food) do not become “saturated” as quickly, if ever. Secondly, the technology is continually changing and improving due to miniaturization and hybridization. Handsets are becoming smaller while increasingly incorporating: MP3 players, video, PDAs, SatNav, Internet, TV and other capabilities. This keeps the price of some handsets, and hence the theft incentive, extremely high. In May 2006, a Nokia 8800 handset cost £546.75 from a popular online retailer. It was worth a third of its weight in gold! (Even after recent increases in the price of gold).<sup>1</sup> Even lower-value handsets are worth stealing for overseas markets where prices can be higher and there is heavy demand. In countries where the market is rapidly expanding but there is no subsidy on handsets, a stolen UK handset is in effect a subsidized handset. Note that whereas the UK had over 100 per cent market penetration (subscriptions *per capita*) by 2005, the rate in many countries was far below that – estimated at 48 per cent in Albania, 34 per cent in Algeria, 25 per cent in Azerbaijan, seven per cent in Bangladesh, 36

per cent in Belarus, 29 per cent in China, 18.5 per cent in Egypt, nine per cent in India, 13.5 per cent in Indonesia, 10.5 per cent in Nigeria, 16.8 per cent in Pakistan, 78 per cent in Poland, and 58 per cent in Turkey.<sup>2</sup> Yet subscription rates in other countries are rising rapidly. Two anecdotes will help illustrate aspects of the international market. First, a survey of customers in Russia showed Motorola handsets to be the most popular – yet Motorola did not retail in Russia at the time! Secondly, a network operator in a country which shall remain unnamed remarked to a seminar audience that his company’s entire business plan was based upon the fact that customers could easily acquire stolen handsets!

## Prospects

Clearly, networks are taking some strides to tackle remaining implementation issues relating to the blacklisting of handsets. There could be a role for NMPCU as an independent monitor to ensure blacklisting rates remain high across networks. It would be preferable if this were not a regulatory move but was undertaken in collaboration with the industry. Improvements to the security of handset IMEI-identities also needs to stay one step ahead of would-be reprogrammers.

Another potential avenue to be explored is the removal of illicit duplicate IMEIs from the networks. This would mean that reprogrammed handsets would no longer work. The technical requirement is that it is possible to identify which duplicates on the network are illicit. In cases where there is only one duplicate and one licit IMEI, the earlier one is almost certainly the licit one. There can be confusion if a user switches the SIM card in the same handset, as it could look like two handsets on the network (thus flagging a possible theft). In instances where a single IMEI has been used for many reprogrammed handsets, the clump of identical IMEIs should stand out. Such clumps can be distinguished from cases where, say, a repair shop tests multiple SIM cards in a single handset (since these would all appear at the same location). Operators may be concerned about the small risk of blacklisting a legal handset, but this can be avoided by the comparison of usage patterns: Calls within a few minutes from the same IMEI in two radically different locations are not because somebody has switched the SIM card! There are certainly ways to avoid passing problems to consumers – a text to notify imminent blacklisting would trigger a free customer service call from any legal users. Moreover, Vodafone Ireland appear to have successfully removed illicit IMEIs from their network, and we are in the process of exploring their means of doing so at the time of writing.

There is a clear need for further research on the extent and nature of the international shipment of stolen UK handsets. Evidence of the nature of the problem could be used to encourage further international use of IMEI blacklisting. The international IMEI database platform, the Central Equipment Identity Register (CEIR), hosted by the GSM Association, is a key player. It is capable of exchanging blacklisting information between networks

1. At 10pm BST on May 10, 2006, the price of gold in the UK was £12.20 per gram – see [goldprice.org/gold-price-uk.html](http://goldprice.org/gold-price-uk.html). Weighing 134g, the Nokia 8800 was worth £4.10 per gram (Source for mobile phone price: [www.amazon.com](http://www.amazon.com) on May 10, 2006).

2. Please note that we are not suggesting these are the key destination countries for UK stolen phones but it is a convenience sample to illustrate how difference in market saturation could influence crime trends.

in different countries. There are, to our knowledge, no technical obstacles to its widespread or universal use. The constraint appears to be one of cost, so there may well be a role for governments to play in further highlighting the immense cost of crime incurred by failure to realize the CEIR's potential. It is remarkable that in 1995 the Parliamentary Office of Science and Technology recognized that "global adoption of IMEI blacklists is necessary to truly tackle the issue of theft for resale" yet the CEIR remains grossly under-utilized even in the UK.

There is a need for research in other areas. Thousands of handsets are sitting in lost property rooms in police stations, bus and train stations, cinemas and other locations across the country. A sample survey could identify the scale of these orphaned handsets. The extent and nature of the unblacklisting of handsets requires further examination. The role of bulk thefts from warehouses, trucks and other sources has barely been touched on herein, but these numerically fewer crimes account for a vastly disproportionate number of stolen handsets. Our preliminary examination of data from Leicestershire police suggests that bulk thefts may be less than one *per cent* of crimes but account for more than a quarter of handsets stolen. Further secondary analysis of police data and British Crime Survey data may provide useful information on patterns and trends that could inform prevention. And although only a relatively small proportion of handsets appear to be insured, reduced crime is clearly in the interests of insurers. Providing them with the requisite technical and other information would surely allow them to nudge the industry into further crime prevention activity.

### Concluding Note

Though we have sought to chart progress in crime prevention to date and to suggest there are prospects for further change, others have expressed cynical views of the pace and extent of change. One commentator wrote:

"[T]here remains a disquieting feeling that operators and handset makers are dragging their feet, focusing more on revenue from calls and future sales (victims need to get new phones) than customers' frustrations."<sup>3</sup>

3. James, J. 2002. "A call for help" *Time Europe*, March 4, 2002 (at [www.time.com/time/europe/magazine/article/0,13005,901020311-214207,00.html](http://www.time.com/time/europe/magazine/article/0,13005,901020311-214207,00.html), accessed December 2005).

Arguably the most frustrating aspect of preventing mobile phone theft is the seemingly slow pace of development and implementation of crime prevention efforts. It is not an easy task. On one hand, altering the operations of network operators could be likened to turning around an oil tanker – it takes time and effort and requires patience. Yet on the other hand, we know these to be hotly competitive businesses that react with lightning speed to changes in the market. Perhaps Victim Support and the international victims' lobby should push for further measures. The prospects for crime prevention would be greater if market forces could be harnessed to instil a sense of urgency, and market-based incentives are preferable to regulation. But otherwise, like it or not, we cannot particularly blame the mobile phone industry for focusing on profits even if crime is an inadvertent by-product. Perhaps performance league tables on stolen handsets and blacklisting rates, akin to those which stimulated security in the car industry (the Home Office's car theft index), would provide consumers with greater information.

The costs of crime due to handset theft are far greater than the money cost of handset replacement. They include physical injury incurred during the course of a robbery, the emotional cost of being a victim of crime, and the time, effort and inconvenience involved in losing and replacing a phone. The costs to society include lost productivity if victims take time off work (to recover or to arrange replacement), the cost of business from lost telecommunications and information, the cost of health services, the cost of insurance administration, and the cost of policing and criminal justice services. Our preliminary estimates suggest the costs of mobile phone theft in the UK are, at minimum, around £1 billion *per annum*, and perhaps as much as £7 billion (depending on which estimates and methods are used). It behoves us to press for continuing and sophisticated prevention efforts.

### Acknowledgements

This information was collated as part of an ongoing research project funded by the Engineering and Physical Sciences Research Council and the project team includes Ian Storer and John McCardle of the Department of Design and Technology at Loughborough University.