

Article

# MOBILE PHONE REPROGRAMMING: ITS EXTENT AND PREVENTION

**Tulay Kaplankiran, Jen Mailley,  
Shaun Whitehead and Graham Farrell**

Loughborough University, Loughborough, UK

Correspondence: Graham Farrell, Midlands Centre for Criminology and Criminal Justice,  
Loughborough University, Loughborough, LE11 3TU, UK. E-mail: g.farrell@lboro.ac.uk

## Abstract

*Reprogramming involves hacking the software of a mobile phone to change its identity. A handset's international mobile equipment identity number (equivalent to a car's vehicle identification number) is altered to enable illegal re-sale, thus facilitating theft and robbery of mobiles. The extent of the problem has not been adequately measured and so this study presents two approaches. The first was an on-street survey of owners that examined their mobile phones. The second was an examination of mobile phones in lost property offices. A conservative estimate is that 5% of the sample of mobiles were stolen or reprogrammed. Studies with larger representative samples are needed but, if representative, this suggests that millions of stolen/reprogrammed mobiles are in circulation in the UK. Possibilities for policing and prevention are discussed.*

## Keywords

mobile phone theft; reprogramming; stolen goods

*Crime Prevention and Community Safety* (2008) 10, 271–279.

doi:10.1057/palgrave.cpcs.8150060

## Introduction

**W**hen stolen cars are given a fake identity, they are colloquially known as “ringers”. Stolen mobile phones with a fake identity are also ringers, but the term “phone ringing” seems unlikely to



catch on in this context. However, just as the ringing of cars is a facilitator of car theft, so too reprogramming of mobile phones is a facilitator of robbery and theft. The subject warrants more research attention than it has received to date.

Mobile phone theft increased rapidly in the mid to late 1990s. Harrington and Mayhew (2001) estimated that by 2000 there were 710,000 annual mobile phone thefts in the UK. Hoare (2007) estimated 800,000 victims of mobile phone theft in the years 2005 and 2006. The level and seriousness of mobile phone theft became increasingly apparent in a decade when many other types of crime were decreasing (see Jansson *et al.*, 2006). The causes of the increase were the rapid increase in mobile phone ownership and the characteristics of phones that made them attractive targets. According to Ofcom, by 2006 the number of mobile phones connected in the UK had exceeded the population for the first time. There have been some successes in tackling crime relating to phones. Clarke *et al.* (2001) described how cell phone fraud in the US was significantly reduced by technological innovation by the phone industry. Other measures taken by police and industry in the UK include the street crime initiative and the immobilize campaign, described elsewhere (Mailley *et al.*, 2006a).

The mobile phone market is fast moving and dynamic, with customers frequently upgrading their handsets, and manufacturers maintaining high prices by introducing new models with new integrated technologies. Hybridization, including the incorporation of digital cameras, PDA facilities, MP3s and, increasingly, SatNavs and TV capabilities, maintains retail prices and serves to continually stimulate demand in the black market for stolen handsets. In this context, the reprogramming of stolen mobile phones is a key facilitator of mobile phone theft.

The aim of car ringing and phone reprogramming is the same. It is to change the identity of a product in order to mask its illicit origin. Cars have a unique vehicle identification number (VIN) etched onto a plate on the door, in the engine bay and chassis. Forged VIN plates and chassis are used to pass a stolen car as legal so it can be sold. Similar to the car's VIN, a mobile phone has a unique international mobile equipment identity (IMEI) number that is stored in the handset's software. The handset IMEI is also found on a plate (usually a label) located under the battery. The software storing the IMEI can be hacked so that the IMEI can be altered. The stolen handset is given the IMEI identity of a legal mobile. This means that, even if the stolen mobile has been reported stolen and blacklisted by phone networks via its original IMEI, the new IMEI then passes network log-on checks. Just as a "ringer" car enters the legal pool once again, so the reprogrammed handset will be able to access phone networks even if its previous software identity had been blacklisted. Preventing reprogramming is therefore a potential means of reducing mobile phone theft and robbery.

## Current prevention efforts

Currently there is a twofold approach to tackling the problem of reprogramming:

- Detecting and prosecuting reprogrammers.
- Increasing the security of handset software to make reprogramming harder.

The Mobile Telephone (Reprogramming) Act 2002 made phone reprogramming illegal. The Act was passed because the police believed the problem was extensive. Colleagues at the National Mobile Phone Crime Unit (NMPCU) have countless stories of sting operations, reprogrammers and reprogrammed mobile phones.

Mobile phone manufacturers have made some effort to reduce reprogramming. The mobile industry's trade association, the GSM Association, published "9 principles", to encourage manufacturers' security concerns (GSMA, undated a). Changes in IMEI security are monitored via a "Weakness Reporting and Correction Process" (GSMA, undated b), the results of which do not appear to be publicly available. There are now some phone handsets that store the IMEI in a one-time programmable, non-rewritable, memory chip (termed a "UEM" chip). Since, in theory, it cannot be re-written, replacing the chip is the only option. There are possibilities to integrate the chip with other aspects of handset circuitry such that removing the chip results in the phone being incapacitated. At the same time, however, it is also likely that kits and parts will become more readily available, and cheaper, particularly via the internet. This will allow offenders to replace the chips themselves, enabling them to reprogramme the new chip with any IMEI that they wish. At the time of writing in late 2006, some online forums suggest that ways are being found around these security measures.

In short, however, efforts to stem reprogramming have been, at best, mixed. Critically, the extent of reprogramming remains unknown, and therefore its overall significance is unknown. The present study explores methods that seek to fill this gap in knowledge.

## Survey measures

This section describes the two surveys undertaken to measure the extent of mobile phone reprogramming. The principle underpinning both surveys was an identity check of phone handsets. Determining whether a mobile phone has been reprogrammed is conceptually simple. The IMEI, the equivalent of the car's VIN, is a 15-digit number unique to every mobile phone. The number is located in two places on every handset. The first is stored in the software. This number is displayed on the screen when \*#06# is typed into the keypad. The

second “hard” copy is etched onto a number plate, which is a label. The label is normally located under the battery inside the back of the phone. Sometimes the hard copy is not specifically identified as the IMEI but is just a line of numbers, and often it is quite small lettering and tricky to read. To overcome this, the police NMPCU issue magnifying glasses to their officers. For any given handset, the two IMEI numbers (software and number plate) should match. If they do not then the identity of the phone has been changed, probably by modification of the software. If the IMEI number plate is missing, then this is an indicator that the phone may have been stolen. It is an indicator of theft because the number plates are hard to remove, they cannot be accidentally removed, and there is no legitimate reason to remove them. Hence, the only individuals who are likely to seek out and remove the IMEI number plate are those who do so to hide the identity of the handset.

### Survey of owners

Face-to-face interviews with phone owners were conducted in one town and two cities in the UK. To reduce selection bias, every third person who passed the interviewer was approached. The time and day of interviews was varied to reduce possible bias due to those sources. The average interview time was around seven minutes. Since interviewees were to be asked to reveal their unique handset identity number, they were given assurances of confidentiality, and the interviewer carried a university identity card. In addition, the interviewer would only write the IMEI number on a post-it note so that, once it had been checked with the number on the IMEI label, the post-it note could be returned to the interviewee as reassurance that it was not recorded. However, a small number of interviewees terminated the interview after it had begun, usually at the point when they were asked if the IMEI number could be checked. For the most part, the post-it notes proved a remarkably simple way of gaining the trust of respondents.

A total of 200 interviews were completed, of which 101 were men and 99 women. A quarter of the sample were aged under 20 ( $n=48$ , of whom eight were aged under 15), 30.5% were aged 20–25 ( $n=61$ ), around a quarter were aged 26–35 ( $n=46$ ), 15% were aged 36–50 ( $n=30$ ) and 7.5% ( $n=15$ ) were aged over 50. Two-thirds of the sample (66%,  $n=132$ ) identified themselves as White, 22% as Asian ( $n=44$ ), 5.5% as Mixed ( $n=11$ ) and 3.5% as Black ( $n=7$ ). Seven respondents did not own a phone, of whom five were aged over 50 and two aged under 20. The types of phones owned seemed fairly representative of UK phone ownership more generally, with 40% being Nokia, 46% being Sony Ericsson, Samsung or Motorola, and the remainder from other manufacturers, with Siemens the more prominent. This distribution of manufacturers is similar to that found among a recent study of over 100,000 stolen phones (see Mailley *et al.*, 2006b). Among network service providers, 02 were

slightly over-represented relative to the UK as a whole, accounting for 37.5% ( $n=75$ ), Orange, Vodafone and T-Mobile account for 49% combined, 3.5% ( $n=7$ ) by the “3” network, and 6.5% ( $n=13$ ) reporting that they used “other” networks. These “other” networks included CarPhoneWarehouse, Phones4u, Virgin or Tesco, who operate as subcontractors to the main network providers.

Of the 193 phone owners surveyed, 30 declined to disclose their IMEI when that stage of the survey was reached. These respondents are therefore excluded from the analysis. It is not known whether respondents would be more likely to refuse if they had reason to believe their handset might have been stolen at some stage. In two further interviews the phone handset software would not show the IMEI on the screen when \*#06# was entered on the keypad. This left a sample of 161 valid survey responses, which are shown in the first data column in Table 1.

Of the 161 responses, five handsets were found to have IMEI numbers that were different in the software compared to those on the number plate label. These handsets were akin to a car where the licence plate VIN is different from that on the chassis. These handsets are shown in Table 1 as reprogrammed. A further three handsets were found to have had their IMEI number plates removed or defaced. As discussed previously, this is not something that happens by accident, poor maintenance or poor treatment of a handset. Located beneath the battery, the IMEI number plate is not liable to day-to-day damage, does not fall off and cannot be easily removed. Its removal or disfigurement occurs only as the result of purposive action. Realistically, the only reason to remove or disfigure the IMEI number plate is to disguise or hide the true identity of a handset. Moreover, none of the relevant respondents reported that they had removed or disfigured the IMEI number plate. These handsets are listed as “likely stolen/reprogrammed” in Table 1. Hence the main finding of this survey, albeit with a small sample, is that at least 5%, and perhaps 8%, of handsets had been reprogrammed.

At the start of the interview, all respondents were asked whether they were carrying their mobile phones. Four respondents subsequently proved “unable”

**Table 1** Extent of reprogramming found using two survey methods

<i>Finding</i>	<i>Owner survey</i>	<i>Lost property survey</i>	<i>Total</i>	<i>Cumulative percent</i>
Reprogrammed (different IMEIs)	5	1	6	2.8
Likely stolen/reprogrammed (IMEI label removed)	3	1	4	4.7
Possible reprogrammed	5	0	5	7.0
Probably legitimate	148	50	198	100.0
Total handsets	161	52	213	

to locate it on their person. One respondent claimed an inability to open the back of his phone. Since opening the phone is a prerequisite of changing the SIM card, and since the respondent made the claim in a manner that raised the suspicion of the interviewer, there is the possibility that this was an attempt to disguise a phone known to be stolen. These five “suspicious” cases are not counted in the estimate of 5%, but are shown separately in Table 1. If they were included as suspected stolen/reprogrammed phones, then the total would be 8%. This estimate would be higher if the 30 respondents who refused to disclose their IMEI numbers were more likely to have reprogrammed phones than the respondent sample. Hence, it is conservative to conclude that 5% of the sample of handsets was stolen or reprogrammed.

### Survey of lost property

The second measure of reprogramming was a survey of mobile phones in two lost property rooms. Lost mobile phones undoubtedly exist in their thousands in lost property rooms in cinemas, shops, train and bus stations, workplaces, schools and colleges and other locations across the country.

The first source was the lost property office of a mid-sized university campus. Forty-one mobile phones were examined. A key problem was powering-up phones where the battery had died. This reflected the fact that some of this sample may have been in the lost property room for some time. One of the authors (SW) is an engineer who was able to build a makeshift independent power source. As a result, 31 of the 41 handsets could be powered-up. Of these, two were suspected as reprogrammed using the criteria outlined above. One of those handsets had a different IMEI in the software compared to the number plate, and the other had the number plate removed.

The lost property room of the police station in a mid-size market town was the second source of a sample of lost mobile phones. Here, of 42 handsets available, only 21 could be powered-up. Of the 21, none were suspected as having been reprogrammed. However, this is within the margin of error for such a small sample because if 5% were reprogrammed this would only average to one in 20.

The findings from the survey of lost mobile phones are shown in the second column of data in Table 1. Of 52 handsets that could be checked, two, or 4%, were proven or strongly suspected to be stolen or reprogrammed.

Combining the on-street and lost property survey, a total of 213 handsets were examined, of which 10, or 4.7%, were reprogrammed or showed strong evidence of being stolen or reprogrammed. A further five were suspected of being reprogrammed but were unproven cases, which, if included, would take the sample of illegitimate handsets to 7%.

Further studies should be conducted with larger samples. However, the 5% estimate was conservative for the reasons described herein. Hence, it seems

reasonable to conclude that there are many, and potentially millions of, illegal phone handsets in circulation. If there were 60 million handsets in circulation, then, if 5% were reprogrammed, this would amount to three million handsets.

## Prevention

There is scope for further research into the prevention of mobile phone reprogramming. Sources in the NMPCU have suggested to the current authors that stolen mobiles are increasingly “broken” or “chopped” for parts. This is in parallel with cars that are “chopped” and the valuable parts sold separately. Phone screens appear particularly valuable and in some cases account for half the value of a handset. Perhaps valuable components could be etched with the IMEI number just as car parts are etched with VIN numbers. This would allow the police or potential customers to verify the IMEI against a registry of stolen phone identities.

Some stolen mobiles, as with valuable cars, are shipped overseas for re-sale. There is a need for international cooperation, particularly on blacklisting by networks. How is it that fast-moving global manufacturers can coordinate the global roll-outs of new models, yet cannot coordinate the transfer of information for international blacklisting? The mobile phone industry is said to suggest that it is the responsibility of national governments to ensure this transfer of information.

All cars on the road in the UK are required to undergo an inspection to obtain a certificate of roadworthiness or MOT. The MOT system is not infallible but acts as a constraint on stolen, un-roadworthy or otherwise illegal cars. Something similar for mobile phones could reduce reprogramming, increase consumer responsibility and drive some thieves out of the market. More stringent measures could be envisaged: An amnesty could precede legislation that punishes anyone found using a stolen and reprogrammed mobile phone.

There may be scope for random spot checks of mobiles. Drink-driving incurs random checks so why does the same rationale not apply to carrying stolen goods? The victim of a robbery may have experienced significant emotional and physical as well as financial costs. Random spot checks would incentivize both sellers and customers to avoid stolen mobiles.

It is increasingly common for the police to recuperate the proceeds of crime. Recovering the profits made by networks from calls on stolen mobile phones seems reasonable in this context. This would promote corporate social responsibility among network providers, and incentivize them to avoid stolen handsets. The possibility for networks to examine duplicate IMEIs on their systems, a possible indicator of a stolen phone, has been suggested elsewhere, and one socially responsible network obliged stores that had sold stolen handsets to provide replacements to customers (Mailley *et al.*, 2006a). Perhaps there is

the possibility to trace organized crime reprogramming groups via duplicate IMEIs on phone networks. They may be more likely to be those involved in other types of organized crime.

Handset security is currently not particularly marketable. The recent phone theft index (Mailley *et al.*, 2006b, 2008) may go some way toward remedying this. Other possibilities may exist. If safety ratings for individual handset models could be generated, perhaps they could be published by *Which?* magazine, and used to incentivize the security market. There could be ratings for handset IMEI security and for network blacklisting rates (the likelihood that a network disconnects a handset reported as stolen). Such indicators could be monitored by an independent agency such as NMPCU. Over time, customers would switch to more secure handsets and “safer” network providers with stragglers driven out of business.

The poorly designed car known as the Ford Pinto was found to be the cause of death of some occupants during a collision (see Cullen and Maakestad, 1987). There is evidence, documented by the Mobile Industry Crime Action Forum and NMPCU, that network service providers have historically failed to blacklist a significant proportion of mobile phones, thereby arguably facilitating re-sale and encouraging further crimes. There is also evidence that networks allow reprogrammed phones to make calls despite the fact that it may be simple to identify and disconnect them. There are a range of anti-theft devices now on the market for mobiles, including biometric locking of handsets, and remote proximity alarms (where the handset sounds an alarm if removed more than a certain distance from a paired tag carried by the handset owner). To what extent is it justifiable for manufacturers to leave this security out of the manufacturing process? The history of car security suggests that some legislative effort, prompted by victim advocacy and consumer rights groups, may be a key means of ensuring that security and safety measures are implemented (see Newman, 2004). In the UK market, however, handset costs are often highly subsidized by network providers. If customers were obliged to pay the actual cost of handsets, it is possible they would be less likely to leave them prone to theft, and customers may also be more amenable to paying extra for prevention.

## Conclusion

Two survey methods were used to estimate the extent of mobile phone reprogramming. There is a need for studies with larger sample sizes than the ones developed here. However, the estimate that 5% of handsets are reprogrammed may prove to be a conservative one. It is not unreasonable to conclude that there are millions of stolen and reprogrammed handsets in everyday use in the UK, disguised as legitimate handsets. There are a range of potential avenues to explore in relation to policing and prevention.

Changing the identity of stolen products is a major issue for crime prevention and community safety. Unique identification should be an aim for manufacturers of all valuable products. With unique identification, possibilities exist for tracking, detection and deactivation of stolen items. Reprogramming in various forms is then the tactical displacement issue that needs to be overcome. The lessons from cars and mobile phones may prove vital for the furtherance of efforts to prevent the theft of other types of valuable goods.

## Acknowledgements

This research was partly funded by The Engineering and Physical Sciences Research Council under Grant EP/C52036X/1.

## References

- Clarke, R.V., Kemper, R. and Wyckoff, L. (2001). Controlling Cell Phone Fraud in the US: Lessons for the UK 'Foresight' Prevention Initiative. *Security Journal*. Vol. 14, pp 7–22.
- Cullen, F.T. and Maakestad, W.J. (1987). *Corporate Crime under Attack: The Ford Pinto Case and Beyond*. Cincinnati, OH: Anderson Publishing.
- GSMA (undated a). *Security Principles Related to Handset Theft*. GSMA and EICTA. EICTA ref 04cc100.
- GSMA (undated b). *IMEI Weakness Reporting and Correction Process*. GSMA and EICTA. EICTA ref 05mt101.
- Harrington, V. and Mayhew, P. (2001). *Mobile Phone Theft*. Home Office Research Study 235. London: Home Office.
- Hoare, J. (2007). Mobile Phones: Ownership and Theft. In Flatley J. (ed.) *Mobile Phone Theft, Plastic Card and Identity Fraud: Findings from the 2005/6 British Crime Survey*. Home Office Statistical Bulletin 10/07. London: Home Office.
- Jansson, K., Coleman, K. and Kaiza, P. (2006). Violent Crime. In Walker A., Kershaw C. and Nicholas S. (eds) *Crime in England and Wales 2005/06*. Research Development and Statistics Directorate. London: Home Office.
- Mailley, J., Whitehead, S. and Farrell, G. (2006a). Progress and Prospects in the Prevention of Mobile Phone Theft. *Justice of the Peace*. Vol. 170, No. 22, pp 404–407.
- Mailley, J., Whitehead, S. and Farrell, G. (2006b). Bring on the Safety Razor: The Top-10 Stolen Mobile Phones. *Justice of the Peace*. Vol. 170, No. 30, pp 564–566.
- Mailley, J., Garcia, R., Whitehead, S. and Farrell, G. (2008). Phone Theft Index. *Security Journal*. Vol. 21, No. 3, pp 212–227.
- Newman, G.R. (2004). Car Safety and Car Security: An Historical Comparison. In Maxfield M. and Clarke R.V. (eds) *Understanding and Preventing Car Theft, Volume 17 of Crime Prevention Studies*. Monsey, NY: Criminal Justice Press, pp 217–248.