Eur J Crim Policy Res (2008) 14:39–60
DOI 10.1007/s10610-007-9040-9

IN SAFE HANDS: A Review of Mobile Phone Anti-theft Designs

Shaun Whitehead · Jen Mailley · Ian Storer · John McCardle · George Torrens · Graham Farrell

Published online: 27 June 2007
© Springer Science + Business Media B.V. 2007

Abstract Anti-theft designs relating to mobile phones are reviewed. The physical and electronic design of handsets includes visual deterrents, owner-identification, and handset tracking options. The systems design of phone networks includes the blacklisting of stolen phones. Other measures include biometric-locking of handsets, and designs that encourage 'safe' phone use and transportation. Characteristics that promote anti-theft designs are proposed and form the acronym 'IN SAFE HANDS': identifiable, neutral, seen, attached, findable, executable, hidden, automatic, necessary, detectable, and secure. The set of characteristics is presented as a heuristic device to aid designing-out crime from frequently stolen electronic goods.

Keywords Anti-theft design · Crime and design · Mobile phones

Introduction

Mobile phone theft has taken the UK crime scene by storm. From the mid-1990s many crimes in the UK declined significantly (Walker et al. 2006), but mobile phone theft has been an increasing problem (Harrington and Mayhew 2001; Mailley et al. 2006a). This article reviews the various types of anti-theft designs relating to mobile phones. 'Anti-theft design' is here used as a portmanteau term that covers a range of areas including:

- Physical aspects of handset design which influence the way they are carried and used by owners
- Physical aspects of handset design such as iconography and semantics which convey visual cues to potential offenders
- Electronic components of handsets, including relevant elements of RFID and micro-chips
- Built-in anti-theft technology such as biometric scanning devices

S. Whitehead · J. Mailley · I. Storer · J. McCardle · G. Torrens · G. Farrell (✉)
Loughborough University, Loughborough, Leicestershire, UK
e-mail: G.Farrell@lboro.ac.uk

Samsung Exhibit 1023, Page 1 of 22

- Add-on measures or related equipment such as lanyard chains, bespoke carry-pouches and safe pockets
- The design of systems for the management of phone networks, including the policy and practices of network operators

This review does not follow the format of a traditional literature review. That is because of the nature of the subject matter and the diverse sources in which the relevant material was located. Often these took the form of commercial material relating to security, much of it found online rather than in academic journals or reports. The fragmented nature of the literature means it is difficult to claim that this is an exhaustive review. However, if the present study forms a platform for criticism and further work then one of its key objectives will have been achieved. Indeed, the disjointed and informal nature of the source material provides a primary justification for this review insofar as it constitutes a stocktake that, it is hoped, will inform and encourage further effort to design-out mobile phone theft.

The role of product design in crime is now generally recognised (Clarke 1999, 2004; Lester 2001; Gamman and Hughes 2003; Ekblom 2005; Clarke and Newman 2005). To be stolen, a product needs to be both insecure as well as attractive to thieves. In Project Marc, Armitage et al. (in this volume) sought to quantify the security and vulnerability of electronic products in order to inform crime-proofing efforts. The present study is complementary in its approach. Here, the security and vulnerability of only one type of frequently stolen product is examined by mapping the extent and nature of current anti-theft efforts relating to that product. The aim is to provide a platform for the development of additional efforts to tackle the crime problem.

In what follows, an effort is made to discuss generic concepts and designs. However, for illustration and specificity, particular commercial products are discussed in some instances. Where this occurs the intention is that these are representative of their genre rather than promoting any particular brand.

The Characteristics of Secure Products

The structure of this review reflects the framework developed by the research team for the examination of secure product designs. That framework drew upon earlier work examining the characteristics of stolen products, namely the VIVA (*V*alue, *I*nertia, *V*isibility, *A*ccessibility- Cohen and Felson 1979) and CRAVED (*c*oncealable, *r*emovable, *a*vailable, *v*aluable, *e*njoyable, *d*isposable- see Clarke 1999) frameworks. This type of approach has more recently been developed into a crime risk assessment mechanism by project Marc (see Armitage et al. 2006 and other contributions in this volume). Each of those studies identified characteristics which can *promote* the theft of products. However, it is arguable that this is not really what is required for designing-out crime. The other side of the coin, addressed here, is to identify characteristics which can *reduce* the theft of products.

It is proposed that the characteristics of anti-theft designs should include one or more of a set of characteristics, which surreptitiously form the acronym IN SAFE HANDS: identifiable, neutral, seen, attached, findable, executable, hidden, automatic, necessary, detectable, and secure. The characteristics are detailed in Table 1. While IN SAFE HANDS is neither as curt as VIVA nor as catchy as CRAVED, those should be secondary attributes to that of substance. The set of characteristics might be argued to be a theoretical conclusion of the review of product design issues, but setting it out at the front of this article allows us to follow its structure for the review that follows.

Samsung Exhibit 1023, Page 2 of 22

Table 1 Characteristics of secure designs

Identifiable	These are products that are identifiable by their owner. Identification may be, but is not limited to, visual property marking, such as etching, UV marking or licence plates.
Neutral	Anti-theft design features should not adversely affect the user's experience. The feature should not make a product more difficult to handle or carry, or have other adverse consequences (for example, RFID can also be intercepted and misused by criminals seeking to locate valuable products).
Seen (to be protected)	Being seen to be protected promotes deterrence by increasing the perceived risk. House and vehicle security are promoted by flashing lights and alarm boxes.
Attached	A product which is attached, whether spatially or electronically linked, to its desired location or owner, will be safer. Computers fixed to room fittings have this characteristic.
Findable	If lost or stolen, the product can be tracked and found. Tracker, Lo-Jack, and other car trackers allow them to be found. A lost or stolen mobile phone might be found by calling its number.
Executable	The product or device can be deactivated or otherwise rendered useless if lost or stolen, preferably remotely.
Hidden	A product which is hidden about the person or otherwise, and not used in an overt manner. British Crime Survey data suggests 25% of mobile phone thefts involve phones being used or overtly on display at the time.
Automatic	Protection is preferably built-in, the default option, or automated. Credit card PINs are automated, but mobile phone PINcode locks are rarely used. Lack of automation allows offenders to take advantage of apathy or ignorance on the part of user-owners.
Necessary	It is necessary to be the owner, or to possess information or knowledge held by the owner, to use a product. This includes mechanical keys, user codes, and biometric information.
Detectable	Make it obvious that the product is being stolen or has been stolen. The tamper-proof design of some product tags clearly reveal when they have been removed to facilitate shop theft. Exploding ink-dye in money bags means money from bank robberies is easily detected, to the extent that the cash is effectively worthless.
Secure	Product protection should not be easily removable or hackable. The security itself should be securely designed to pre-empt tactical displacement.

IN SAFE HANDS is intended as a 'straw man' set of characteristics. It is fully expected that the characteristics will be refined to provide better use as an aide-memoire to encourage designers to consider security.

Mobile Phone anti-Theft Designs

This review covers a range of design solutions, which vary greatly in scope. Some are remarkably cheap or simple while others are potentially expensive or technically sophisticated. Some effectively require 'universal' application to be effective while others can be, and are, adopted on an ad hoc basis and tailored to individual requirements. Some of the designs may have implications for legislation, policing, the practices of phone users, or for handset manufacturers or network providers. There is also some overlap between issues relating to theft of the phone service and theft of the handset, since preventing the former may reduce the attractiveness of the latter. The mechanism by which crime is prevented also varies greatly among the various design solutions.

The review of design solutions in this section is structured around a subset of the IN SAFE HANDS characteristics - this subset (identifiable, seen, attached, findable, executable,

Samsung Exhibit 1023, Page 3 of 22

hidden, necessary and detectable) effectively describes the characteristic *mechanism* that affords the protection. The remaining characteristics (neutral, automatic and secure) are those that are required for the deterrent mechanism to function without adverse effect on the legitimate user. Although some designs possess more than one preventive mechanism, they are classified below according to their dominant characteristic.

It is also the case that mobile phones are only one product, and other IN SAFE HANDS characteristics may better apply to other anti-theft designs and products. A listing of the anti-theft design solutions relating to mobile phones is given in Table 2. Each item is described briefly below.

Table 2 Mobile phone anti-theft design solutions

1	Identifiable solutions
a)	Simple property marking
b)	Ultra-violet marking
c)	Microdots
d)	Unique soluble markers
e)	Identify-and-return labels
f)	Permanently personalised handset
2	Attached solutions
a)	Attachment to the individual
b)	Fixed-location handsets
c)	Temporary location-based fixtures
d)	Bespoke secure clothing and carry-pouches
e)	Grip-phone
3	Findable solutions
a)	GSM tracking
b)	GPS Ttracking
c)	Radio frequency identification (RFID)-based tracking
4	Executable solutions
a)	SIM blocking and IMEI-blacklisting of stolen phones
b)	Designing legislation to discourage reprogramming
c)	IMEI label design, use and protection
d)	Physical protection of important chips
e)	Possible 'security kite mark'
f)	Use of a global CEIR
g)	Text bombing
5	Hidden solutions
a)	Wearable phone
6	Necessary solutions
a)	Inbuilt key codes
b)	Personalised auto-locking keycode
c)	IButton
d)	Biometrics
e)	Chargelock
f)	IN-charge
g)	Separate headset/earpiece uniquely linked to handset
h)	Theft deterrent jewellery
7	Detectable solutions
a)	Noisy bags
b)	"I am Stolen"

Samsung Exhibit 1023, Page 4 of 22

It is worth noting that the role of this review is primarily that of collating information about anti-theft options. It does not seek to evaluate the relative effectiveness of different existing measures. Such aims are beyond the present scope but could form the subject of further research. Discussions, interviews and questionnaires undertaken with legitimate mobile phone users, theft and robbery victims and offenders, could form the market research to help assess the effectiveness of the various anti-theft design solutions.

After the description of each solution, it will be stated whether the solution exists already or is proposed.

1. Identifiable solutions

Designs options that make mobile phones identifiable to their owner take various forms. It is primarily physical identification systems that are detailed in this sub-section, while related electronic forms are discussed later as 'findable' options.

a) Simple property marking (existing)

Writing or engraving the owner's name and other details on the property is a common crime prevention measure. It is widely used for products other than mobile phones (see e.g., Laycock 1985). Property marking can also reduce ambiguity regarding ownership and can promote the return of lost items. In relation to mobile phones, property marking can also include less formal personal customisation of other forms such as the use of stickers, handset colours and designs (where handset covers can be purchased separately).

b) Ultra-violet marking (existing)

Property can be marked with ink that is visible only under ultra-violet (UV) light. UV marking provides a common form of property marking that has been around for many years. It was observed in Laycock's classic 1985 examination of the role of property marking in deterring domestic burglary.

c) Microdots (existing)

Microdots are tiny (~10s–100s of μm diameter) film particles that have unique codes printed on them. They can be brushed or adhesively bonded onto products. The presence of microdots on an item is not easily detected by the naked eye, but they can be read under a microscope or powerful hand lens. Microdots are now frequently used for parts-marking on cars and other products (see e.g., Katz 2006 for a short review relating to electronic goods; see also StopTheft undated). Uncertainty regarding their presence will increase deterrence while their presence will increase detection possibilities.

d) Unique soluble markers (existing though not widely used)

Property can also be marked by spraying it with indelible and uniquely identifiable liquid, which may also be transparent. 'SmartWater' is a commercial product described as "an aqueous based solution formulated with a unique forensic code" (SmartWater 2006). Each canister of the solution can, in effect, be identified with the accuracy of DNA. It comes in various forms and can be combined with microdot technology or embedded into the adhesive of tamper-resistant labels.

As well as identifying a stolen product, and therefore its owner, traces of SmartWater on an individual can be used to link them to the scene of a crime. Its crime prevention and detection potential have been outlined elsewhere (Farrell 1997) though they have not, to our knowledge, been formally evaluated (see also Andrews 2005).

e) Identify-and-return labels (existing)

Other forms of property marking involve more formalised systems for identifying and returning property to owners. Trackitback (see Trackitback 2005) is a commercial example of a product labelling-and-return scheme. Clients purchase labelling packs and affix the

Samsung Exhibit 1023, Page 5 of 22

Fig. 1 'Trackitback' label on the front of a handset

unique identification labels to their valuables. The details of the valuables are registered on the website and linked to the label identification number (Fig. 1).

When a registered item is lost, the ID label instructs the finder to contact Trackitback, and a reward is offered for the return of the item. The return of items is coordinated through Trackitback. The anonymous ID numbers and returns system mean that the owner and finder do not meet and their personal information is not revealed. The system can also be used by police or others to return lost items.

f) Permanently personalised handset (proposed)

It is possible to conceive of individually personalised handsets. Though this is not, to our knowledge, an existing commercial effort, the concept is a formalised version of the frequent practice that individuals have of personalising their handset. Informal personalisation often takes the form of labelling and stickers. Customised handset facia or covers are widely available for many popular handset models, but they are still generic rather than individualised. A unique personalised facia could conceivably include a custom-made design including moulding and colour scheme. It could also include personalised names or a personal tag, that is, some form of clear property marking, as part of the design or engraved on a handset. Designs could be registered on a database, and new facia/covers could be (semi) permanently bonded to a handset. This possibility is offered here as a concept that would formalise many common practices and seek to maximise the anti-theft component of product personalisation.

2. Attached solutions

Mobile phones that are attached, whether physically or spatially, to their owner or desired location, will produce less temptation for theft as they will not appear unattended.

a) Attachment to the individual (existing)

A chain or lanyard attaches the mobile phone to the body or clothing of the user. If the chain is visible it may act as a deterrent (although conversely, any ostentatious use could attract attention to the user of a valuable phone). More practically, the chain reduces the likelihood of a user facilitating or encouraging theft by accidentally leaving the handset unguarded. This is the advantage over the common practice of carrying a mobile phone in a pocket or bag where it does not have a physical attachment. A chain would also increase the

Samsung Exhibit 1023, Page 6 of 22

time and effort required for a sneak-theft or snatch-theft, and possibly reduce the temptation for a robbery. The phone remains portable and moves with the user, being fixed to the individual rather than a particular location.

A mobile phone handset can be conceived where its attachment to the user is in-built as part of its design. A wrist-phone, of a similar style and use pattern to a wrist-watch, would be strapped to the user. Although valuable wristwatches are sometimes stolen from individuals during robberies, they are seldom taken during snatch thefts, and more rarely left inadvertently unattended. The concept design shown as Fig. 2 was developed by Andrew Midgley of the Department of Design and Technology at Loughborough University.

b) Fixed-location handsets (proposed)

A mobile phone can be fixed to a particular location rather than an individual. The attachment could be via a simple chain or other means. This possibility is not in contravention of it being a 'mobile' phone. It is preferable to think here of the phone being wireless, and of its possibility for being located in areas which do not have landline connections. Hence, despite the apparent oxymoron it is possible to conceive of a fixed-location mobile phone in instances such as bars, restaurants, institutions or other locations - in the same way that pens are fixed to the counter in banks and post offices. This brings the benefit of a wireless network while recognising that a handset should not be moved from a particular location, reducing the temptation and opportunity for theft.

c) Temporary location-based fixtures (existing)

The Chelsea Clip is a hook for bags or other items (see e.g., Selectamark undated). It is fixed to tables, walls, bars or other areas in public places from which items are frequently stolen. Chloe Smith and colleagues (2006) examined theft in bars and found that mobile phones are taken in a minimum of 9% of thefts (when they were the only unattended item taken). If a mobile was taken in only half of handbag thefts they were taken in 26% of bar thefts (Smith et al. 2006, p. 11; Table 3). The Chelsea Clip is intended to protect the belongings of citizens and customers by deterring snatch thefts. It is made from tough material to resist efforts to break it. The clip combines elements of attaching the handset to an individual and to a location. It temporarily fixes a phone (or the bag in which it is located) to a location, while allowing it to relocate with the individual as necessary.

d) Bespoke secure clothing and carry-pouches (existing)

It is normal practice to carry a mobile phone in a pocket or a bag. In many instances this is a significant anti-theft strategy as the phone is concealed, reducing temptation, and increasing thieves' uncertainty about whether an individual has a phone and where it is

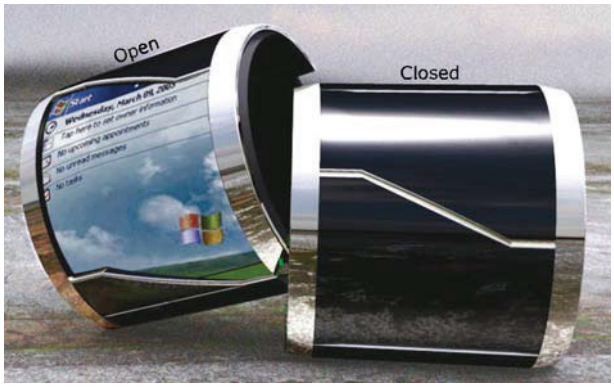

Fig. 2 Locking wristband mobile phone concept

Samsung Exhibit 1023, Page 7 of 22

located. However, a range of bespoke 'secure' clothing and accessories have developed with the aim of reducing the various types of theft. Many thefts from the person involve either snatching or lifting, dipping (into bags or jackets) or slashing (of bags to gain access to contents). Different aspects of designs, particularly those relating to bags, address these particular features of theft.

Specialised carry-pouches can include waist-bands. They are a similar concept to the waistbands often used by tourists to conceal and carry passports safely, but adapted here to carry phones (and other valuables). Likewise, at least one wristband has been developed that allow the users to transport a mobile phone handset which is, in effect, strapped to their wrist (see e.g., Karrysafe undated- see Figs 3 and 4).

e) Grip-phone (proposed)

There may be some scope to improve the ergonomic design of phone handsets in ways that encourage of facilitate 'safe' carrying by users. A 'grip phone' (illustrated in Fig. 5 as developed by the Department of Design and Technology of Loughborough University) is conceivable which is designed to naturally and comfortably interlink with the hand.

3. Findable solutions

If a product can be tracked and found when stolen then this is likely to reduce the rewards of crime, and reduce the incentive for its commission. While a lost phone might be found by calling its number (if it is found by a cooperative citizen), other methods are required to track and find stolen phones.

a) GSM tracking (existing)

The mobile telephone network is divided into Global System for Mobile communications (GSM) cells. Each cell is formed by the area of coverage of a base station. It is possible for several base stations to make contact with a handset at any time. Calculations based on the timing and signal strength of the communication between the phone and the base station can be used to 'triangulate' an approximate position for that particular handset (illustrated in Fig. 6).

This information can then be processed by a geographical information system (GIS) to provide real-time information on a map or as text, to be accessed via the internet or even via another mobile phone.

Currently, systems work with most, but not all UK network operators. The facility is being phased into the 3G network. GSM tracking systems can be accurate up to 50m in urban areas where base stations are numerous, but may be accurate to less than 10km in rural areas. (Vodafone has developed the 'Timing Advanced' mobile phone tracking system that promises to make phone tracking up to three times more accurate). Of course, where no signal is available the phone cannot be tracked at all. GSM-based tracking systems are becoming increasingly popular for tracking delivery and service vehicles and personnel, and for enabling parents to monitor the location of their children.

Fig. 3 Karrysafe 'bodysafe' pouch

Samsung Exhibit 1023, Page 8 of 22

Fig. 4 Karrysafe 'phonesafe' wristpouch

b) GPS Tracking (existing)

Where greater accuracy is required, a global positioning system (GPS) mobile 'phone-based' system can be used. This is more expensive than a GSM system, but as the devices use precise navigation data from a series of satellites, locations can be identified to two metres or less. Increasingly, smart phone handsets such as the Mio A701 have GPS systems built in (see e.g., Smith 2005). For tracking, the phone can be set to transmit its GPS-derived location.

Fig. 5 Grip-phone concept

Samsung Exhibit 1023, Page 9 of 22

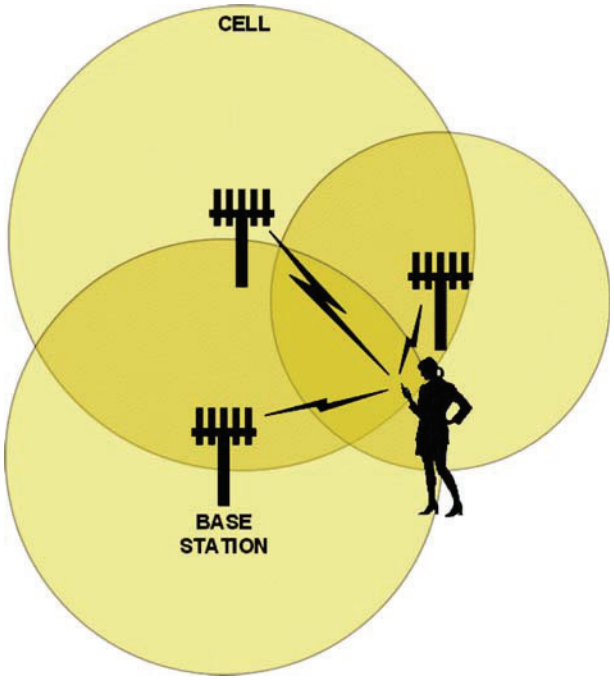

Fig. 6 Triangulation via GSM cells

GSM and GPS tracking systems are already being used as security devices. Makeshift and proprietary systems using phones or GSM units are hidden within vehicles, so that the vehicle can be tracked when stolen. Popular commercial applications relating to mobiles include those of MapAMobile (undated), Childlocate (undated), AccuTracking (undated), FollowUs (undated), Findyourchild (undated) and, TraceAMobile (undated).

It is worth noting that the European Union has invested a large amount of money in the Galileo satellite system. This series of satellites for navigation should be complete by 2010, and will be a rival to the US GPS system. There are likely to be increasing opportunities and incentives in Europe for designers and manufacturers to incorporate Galileo satellite navigation features into consumer devices.

c) Radio frequency Identification (RFID)-based tracking (proposed)

RFID is an automatic identification technology whereby digital data encoded in an RFID tag or "smart label" is captured by a reader using radio waves. An RFID device is illustrated in Fig. 7.

RFID is similar to bar code technology, but does not require the tag or label to be seen to read its stored data. RFID works over short range, (typically measured in centimetres). RFID tags are increasingly being used on pallets and individual items for stock control (see Beck 2006 for an excellent review). RFID reader add-ons for mobile phones are already on the market. An evolution of RFID is near field communications (NFC) technology (see Economist 2005). NFC is particularly directed at mobile electronic devices. NFC works on exactly the same principle as RFID; however, it is generally designed to communicate at extremely short distances, that is, in close proximity to a reader. NFC exchanges more interactive information between the device and reader, and as such is linked to the mobile phone software, unlike RFID tags that are generally ‘dumb’. With appropriately placed

Samsung Exhibit 1023, Page 10 of 22

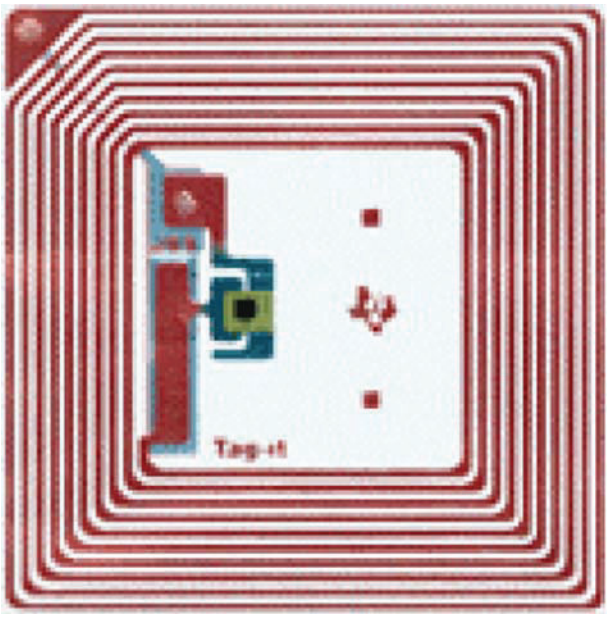

Fig. 7 RFID device

readers, it is possible to track the movement of RFID-tagged and NFC devices for security and crime-prevention purposes.

4. Executable solutions

If a mobile phone can be deactivated or otherwise rendered useless if lost or stolen then it is 'executable'. Such a solution, if properly implemented, would reduce the rewards to phone theft and thus reduce theft, even though a theft itself is not necessarily harder to commit.

a) SIM blocking and IMEI-blacklisting of stolen Phones (existing)

When a mobile phone is reported stolen, it is possible for the network operators to remotely block the use of the SIM card or the handset itself. A handset is blocked ("blacklisted") via its unique serial number, the International Mobile Equipment Identity (IMEI) which the handset uses to identify itself when logging-on to a network. This is a potentially very powerful solution to mobile phone crime, particularly if enhanced by widespread promotion of the technology, coupled with design and styling work.

However, there are few if any technological obstacles to overcome. The problems that remain relate to implementation. For example, at the time of writing a recent report showed that network providers often failed to blacklist stolen handsets (System Concepts 2005).

Possible enhancements to the existing blacklisting process include the following:

b) Designing legislation to discourage reprogramming (existing/proposed)

Design and legislation must be inextricably linked in efforts to reduce mobile phone theft. In particular, legislation can be used to promote crime reduction incentives that stimulate anti-theft design. If owning a reprogrammed handset was an offence this would surely stem illicit resale markets. Such a shift to *caveat emptor* would discourage would-be customers from

Samsung Exhibit 1023, Page 11 of 22

seeking out or passively accepting illegal sales from both online and physical outlets. If selling a reprogrammed handset was also an offence this would massively increase the risks to fences who could be reported by consumers who, due to their own liability, are overtly checking the identity of handsets. The principal legislative reference point in the UK is the Mobile Telephones (Reprogramming) Act (2002) but it does not contain elements such as those suggested here to encourage anti-theft designs by stimulating the market.

c) IMEI label design, use and protection (proposed)

Currently, a handset's unique identifying IMEI number is printed on a label, typically hidden under the battery pack. Few people are aware of its location and fewer still check its validity against the IMEI stored electronically in the handset. Removing, defacing or otherwise tampering with a handset IMEI identifying label could be made an offence. There is not, to our knowledge, any legitimate reason for such activity. It is a means of hiding the identity of a reprogrammed handset and, thereby, a means of facilitating theft. It is akin to seeking to erase the VIN number from stolen vehicle parts to hide their identity. In large part, the mechanism by which this type of legislation would reduce crime is via the uncertainty and perceived increase in risk that it would generate, which would produce a deterrent effect significantly greater than the actual risk.

d) Physical protection of important chips (proposed)

It seems likely that efforts to prevent the reprogramming of IMEIs (for example by storing the IMEI in a one-time programmable (non-rewritable) memory on a UEM chip) will be increasingly successful at deterring simple reprogramming. However, it is also likely that kits and parts will become more readily available, and cheaper, which allow the criminal to replace the chips themselves, enabling them to reprogram their new, pristine chip with any IMEI that they wish. To stay one step ahead of the determined criminal, some means to physically prevent these chips being replaced should be considered. One concept, although we do not have the means to explore it further here, would be a tamper-proof design wherein removing the chip further damaged the handset or otherwise rendered it useless.

e) Possible 'security kite mark' (proposed)

Market forces must be considered as an integral part of the design process. If the handset manufacturer and network operator are in need of an incentive to make handsets and operator processes more secure, it is possible that the equivalent of the British Standards Kitemark could be used to identify those handsets/network operator processes that are known to offer the best in security design features at the time of manufacture. Such an award might well give the manufacturer/network operator a competitive edge in an age when many handsets and networks have little to differentiate them otherwise. The mark could also be a useful means of making consumers aware of security when making purchasing decisions.

f) Use of a global CEIR (proposed)

Currently, a software platform (the Central Equipment Identity Register) exists for the international exchange of blacklisting information (so that handsets blacklisted in the UK cannot be used abroad). However, the international database is rarely if ever used. The consequence is that phones blacklisted in the UK will still work abroad, with the result that there is an apparent increase in the international trafficking of mobile phones stolen in the UK. It is conceivable to 'design' a system of incentives or legislation that will link the various national equipment identity registers to allow almost global blacklisting of all stolen handsets. There is also a possible alternative to relying on the global CEIR to reduce international trafficking, which could be based on a handset 'country lock'. This would mean a handset could only use a SIM-card from its own country. However, this introduces other issues that would need to be explored in detail and cannot be addressed in the space available here.

Samsung Exhibit 1023, Page 12 of 22

g) Text bombing (existing)

Text bombing has been trialled by the Dutch police in Amsterdam. 'Bombing' involves bombarding stolen phones with a continuous stream of messages that effectively preclude normal phone use (as discussed by Harrington and Mayhew 2001). The mechanism by which it works is 'denial-of-service' akin to that sometimes used by offenders to block communications by overloading it.[1]

5. Hidden solutions

A hidden solution is where a mobile phone is hidden about the person or otherwise concealed. Hidden would also include design options which mean that a phone is not used in an overt manner. As phones have become smaller and lighter they can more easily be concealed. The large brick-like early mobile phones, such as that sported by comedian Ernie Wise in Fig. 8, would not fit particularly easily into most purses or the pocket of a pair of jeans. However, the solutions addressed in this section are special efforts at designing-out exposure rather than the more routine precautions.

a) Wearable phone (proposed)

Wearable gadgets are becoming increasingly fashionable. A mobile phone handset that is built into clothing could resist opportunistic and snatch thefts, since it would be difficult to remove, and the owner would be less likely to leave it lying around inadvertently. A concept design mobile phone (developed at Loughborough University Department of Design and Technology) built into gloves is shown in Fig. 9. Wearable phones can potentially be combined with dispersed technology, so that different parts of a phone are worn in different locations on the body. This would frustrate would-be thieves, increasing the time, effort and risk involved in theft. Stealing one component of a dispersed phone would be fruitless if the component had a unique code lock known only to the owner.

6. Necessary solutions

A 'necessary' design solution is where it is necessary to be the owner, or to possess information or knowledge held by the owner, to use a product. Hence such designs include physical and electronic keys and codes, and biometric identification technologies.

a) Inbuilt key codes (existing)

Mobile phones already have security features built in that, if activated, require certain knowledge to be used. There are a number of key codes, including:

i. SIM PIN code (and sometimes SIM Pin Code 2)

The SIM PIN code locks the SIM card. This protects the user's account, even if the SIM is put into another handset. There is often a default code set by the service provider (for example, 0000 on Vodafone, 7890 on Virgin). The SIM PIN code can be changed by the user. If the incorrect SIM PIN code is entered three times in a row, the SIM card will lock up. The network operator must be contacted to obtain a PIN unlock code. If the incorrect PIN unlock code is entered too many times, the SIM will become permanently disabled. Note that this lock does not prevent the handset being used with a new SIM card.

ii. Phone security code

The Phone security code locks the handset itself, not the SIM card. Again, default codes are pre-set, but the code can be changed by the user. It is possible to configure some handsets so that a new SIM card will only be accepted if the phone security code is entered.

[1] Thanks to Paul Ekblom for noting this is denial-of-service used in favour of crime prevention

Samsung Exhibit 1023, Page 13 of 22

Fig. 8 Ernie Wise is alleged to have made the UK's first mobile phone call on 01 January 1985 (source: BBC 2005)

If the incorrect phone security code is entered too many times, the handset will lock up. The network operator must be contacted to obtain a master reset code, which will unlock the handset.

Fig. 9 Concept wearable mobile phone

Samsung Exhibit 1023, Page 14 of 22

b) Personalised auto-locking keycode (proposed)

The existing SIM PIN and phone security codes would be more effective against crime if they were used. A personalised auto-locking keycode could be a next step. An auto-locking code would be activated on a timer, akin to the current keypad locks on some handsets (which serve to reduce expensive accidental 'handbag' calls which can occur when the keypad is inadvertently unlocked). However, whereas keypad locks typically require the next user to type '*' and 'unlock', a personalised PIN-code would be necessary. While more sophisticated thieves or fences would try to find ways to hack the software, some would be deterred, and software security is continually improving.

c) iButton (proposed)

Maxim's iButton® is a computer chip enclosed in a 16mm diameter stainless steel 'button' can (Fig. 10). The button can be attached to a key fob, ring, watch, or other personal items.

The metal casing of the iButton forms an electrical interface, so that when an iButton is touched to another iButton or 'Blue Dot' receptor, the two devices can communicate with each other using the1-Wire® protocol. The Blue Dot can be linked to computers, personal digital assistants (PDAs) and mobile phones, or other equipment. Each iButton has a unique and unalterable address, which can be used as a key or identifier. The iButton can be used to grant its owner access to a building, a PC, a piece of equipment, or a vehicle (see Maxim 2006).

An iButton can hold and transfer similar information to an RFID tag; however, because physical contact between devices is needed for communication, the device cannot be read remotely. This is disadvantageous for certain purposes, for example tracking at a distance, but it does make the device more secure against remote hacking. Despite the possibilities, there appears to have been little global interest so far in the use of iButtons for mobile phone security.

d) Biometrics

i. Fingerprint (existing)

Several mobile handsets featuring fingerprint recognition technology are already on the market at the time of writing (Geoghegan 2005). One example is the Pantech GI100 (see GSMArena undated, and Fig. 11) which will only allow certain functions to be accessed after a registered fingerprint has been recognised.

ii. Face recognition sensors (existing)

Typical of face recognition devices that are becoming available is OMRON's OKAO Vision Face Recognition Sensor (Fig. 12), which can be implemented in PDAs, mobile

Fig. 10 iButton and 'Blue Dot' receptor

Samsung Exhibit 1023, Page 15 of 22

Fig. 11 Pantech GI100 fingerprint scanning handset

phones or other mobile devices with a camera function. There is no requirement for additional hardware. Users register their own face image to their handset with the handset's camera. To use the unit, the user takes his or her own photo, and the sensor software will automatically detect the user and unlock the unit.

Such software is typically designed to work quickly (less than 1 second from taking the image) and tolerant of a wide range of facial orientations. It is also designed to be less demanding on processor and memory requirements (see e.g., Omron 2005).

Fig. 12 Handset using OMRON OKAI vision sensor (Omron)

Samsung Exhibit 1023, Page 16 of 22

iii. Iris/Retina scanning (proposed)

Iris or retinal scans utilise the fact that each individual's retina is unique in the same fashion as each fingerprint. The possibility has been mooted in relation to mobile phones (see e.g., Cho et al. 2006). A user would only have access to the phone if their scan was registered. Sharing handsets would of course still be possible, so long as the owner unlocked the handset before lending it, or scanned their associate's retina into the 'acceptable' set.

iv. Gait analysis (proposed)

Less established forms of biometrics have been mooted in relation to their security possibilities. The use of accelerometers to identify users via their gait, that is, their walking style, is one possibility. At the time of writing, however, such systems appear to be some way from practical application (see e.g., Mantyrjarvi et al. 2005).

e) Chargelock (proposed)

An entrant in the Design Council's Creative Crime Busting Design Challenge (2002), Michael Cross of Sheffield Hallam University proposed the Chargelock, "a device that renders portable electronic products worthless to anyone but their rightful owners, by denying them the ability to recharge the products" (Sheffield Hallam University undated- a). The handset can only be charged by a unique associated charger that is supplied with the phone. The aim is to make it very much more difficult and expensive for thieves to get stolen electronic goods back into circulation. The Chargelock is also intended as a visual deterrent to theft because the handset is seen to be protected with careful use of semantics and iconography - the interface between the charger and phone was styled by Cross to represent a sturdy lock.

f) IN-Charge (proposed)

Another entrant in the Creative Crime Busting Design Challenge was Luke Worrall from Sheffield Hallam University. Worrall designed the IN-Charge system. The device is similar in concept to the Chargelock; however, it specifically incorporates a PIN system linked to an immobiliser (see Sheffield Hallam University undated- b).

g) Separate headset/earpiece uniquely linked to handset (proposed)

This concept is similar in principle to the Chargelock and IN-Charge. Wireless headsets, particularly Bluetooth, are increasingly being used with mobile phones. In this proposed security concept the headset would be uniquely associated with a particular mobile phone handset. Such concepts have been investigated by students in the Department of Design and Technology at Loughborough University.

h) Theft deterrent jewellery (proposed)

Also from the Creative Crime Busting Design Challenge, Billy Greenhalgh from Sheffield Hallam University designed theft deterrent jewellery, seeking to combine secure technology and fashion design. A chip worn on the body as jewellery or a watch is 'read' by the corresponding handset and only when this chip was located would the handset connect or send a text message. The system would work over a small radius and would not affect incoming calls (see Sheffield Hallam University undated- c). This concept could possibly use near field communications technologies.

7. Detectable solutions

If a design solution renders it obvious that a mobile phone theft is occurring, or has occurred, then this is a detectable solution.

a) Noisy bags (existing)

The Karrysafe Karryfront Screamer bag has an inbuilt anti-attack alarm that will automatically start screaming if the bag is removed by force - the force breaks the electrical

Samsung Exhibit 1023, Page 17 of 22

connection in the bag strap, causing a 138dB alarm to sound (see Karrysafe undated, and Fig. 13).

Karrysafe also produces a Scroll Top Backpack, with a noisy Velcro seal that can easily be heard when it is being opened, 'making life difficult for the silent thief' (Fig. 14). The scroll top has a very distinctive red and black 'warning' colour scheme.

After-the-crime detectable solutions:

b) "I am Stolen" (proposed)

A variation on a conventional alarm would be a system that can be automatically triggered or activated remotely, either immediately after an item has been stolen, or at some time in the future. The stolen device would announce that it is stolen by changing colour, flashing a bright light, via a conventional siren or even a voice exclamation. In principle, such a device is akin to the stolen harp in Jack and the Beanstalk, which cries out that it is being stolen, although the giant's response is unsuccessful (see Ekblom 1997, and Everson and Pease 2001 who discuss the repeat victimisation of the giant by repeat offender Jack).

The possibility of the theft being detected and broadcast does not necessarily end with the criminal event itself. Handlers of stolen goods could be dissuaded by the fact that they have no way of knowing if a stolen handset is 'hot' and about to declaim their guilt at any time.

c) Exploding dye pack (proposed)

Exploding dye packs have been used for some time as a crime reduction measure, for example hidden within bundles of notes that are handed over during a bank raid. The permanent dye can be activated by one of several methods, such as timers, movement sensors, or radio remote control.

Other Characteristics

Currently, other desirable features are also being considered for inclusion in the set of 'IN SAFE HANDS' characteristics. In particular, it has become clear that a family of 'reduced value' solutions can be envisaged, typified by 'disposable' and 'ubiquitous' mobile phone concepts, which effectively reduce the potential rewards of theft. Disposable phone concepts have been around for some time, and generally consist of a very basic handset constructed from cheap and recyclable materials, with simple voice and text features. The handsets usually do not have a screen, since the cost of the screen accounts for a high percentage of the manufacturing cost of a mobile phone. Disposable phones, a concept akin

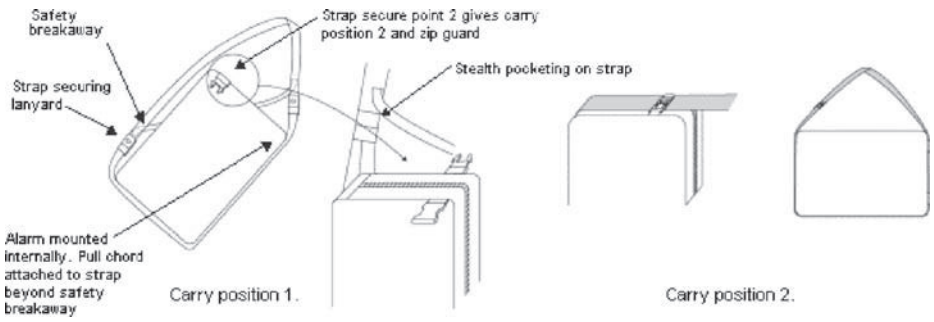

Fig. 13 KarryFront 'Screamer'

Samsung Exhibit 1023, Page 18 of 22

Fig. 14 Scroll Top 'Karrysafe' backpack

to disposable cameras, would be purchased with a small amount of credit, further limiting their value and desirability to thieves.

The ubiquitous phone concept is similar to the fixed-location phone concept presented in Sect. 2b, though as envisaged the handsets could be so dispersed, and of sufficiently low intrinsic value that they would not need to be tied to a particular location.

Discussion and Conclusions

This study has sought to chart the range of anti-theft designs relating to mobile phones. This study is, to our knowledge, the first effort to draw this area together in this manner. Since mobile phone theft has played an increasingly prominent role in UK crime over the last decade, there is a demand for effective and cost efficient anti-theft designs. Recent efforts relating to the car industry have shown that major inroads into crime can be made through design improvements (see e.g., Maxfield and Clarke 2004). Car anti-theft design is believed to have been significantly stimulated by the Home Office's Car Theft Index (see Laycock 2004 for a recent review), and elsewhere the present team have developed a mobile phone theft index as part of the same project research (see Mailley et al. 2006b; Mailley et al. forthcoming). Similarly, a range of advancements have been made in designing out crime from products and systems in other areas (see the collection of studies in Clarke and Newman 2005).

Mobile phone manufacturers and network operators are arguably the agents best placed to further many aspects of anti-theft design. There are clear examples where the potential to

Samsung Exhibit 1023, Page 19 of 22

reduce mobile phone theft has not been realised in the efforts currently managed by the industry. The blacklisting of mobile phones is not nearly as comprehensive as it ought to be, and should be continually monitored by an independent body, such as the police National Mobile Phone Crime Unit. The international coordination of blacklisting is in its infancy despite the fact that there are no known technological obstacles and the software platform upon which such data-sharing would take place has existed for several years. The obstacle seems to be that network providers do not want the bother of transferring data on stolen handsets. Hence, while the system design element has been developed, it has stumbled at the implementation stage. The integrity of handset microchips and software security has improved in response to reprogramming, but at a slow pace. Here there may also be a need for an expert independent monitoring body (see Mailley et al. 2006a for a discussion of a broader range of issues relating to the prevention of mobile phone theft).

The present review was presented around the characteristics of securely designed products. These characteristics, which together formed the acronym IN SAFE HANDS, are viewed by the authors as a heuristic device which it is hoped will stimulate the consideration of security in the process of product design. It is also recognised that the framework is likely to require revision and improvement as thinking in this area develops.

Acknowledgements Funding from the Engineering and Physical Sciences Research Council under grant EP/C52036X/1 is gratefully acknowledged. We thank Paul Ekblom and the editors of this volume for helpful comments.

References

3G (2004). Fingerprint recognition wireless phone, 3G Press Release, 2nd August 2004, at http://www.3g.co.uk/PR/August2004/8140.htm (accessed July 2006).

AccuTracking. (Undated). Low cost GPS services for everyone. http://www.accutracking.com/ (accessed July 2006)

Andrews, R. (2005). Digital Water Marks Thieves. *Wired*, 15 February 2005. Accessed July 2006 at http://www.wired.com/news/technology/0,1282,66595,00.html?tw=rss.TOP

Armitage, R., Clarke, R., Di Nicola, A., Montauti, M., Pease, K., Savona, E. (April 2006). Definition of final crime risk assessment mechanism to measure the risk of theft of electronic products and proof them against theft. Final Report. University College London: Jill Dando Institute of Crime Science. Accessed July 2006 at: http://www.jdi.ucl.ac.uk/downloads/conferences/project_marc/final_report.pdf

BBC (2005). Mobile phones rack up 20 years of use. BBC News online, Saturday 01 January 2005, Accessed March 2006 at http://news.bbc.co.uk/1/hi/technology/4138449.stm

Beck, A. (2006). Shrinkage and radio frequency identification (RFID): Prospects, problems and practicalities. In M. Gill (Ed.), *The handbook of security* (pp. 462–482). Houndsmill: Palgrave Macmillan.

Childlocate (Undated). Childlocate. Accessed July 2006, at http://www.childlocate.co.uk

Clarke, R. V. (1999). Hot Products: Understanding, Anticipating, and Reducing Demand for Stolen Goods. Police Research paper 112. London: Home Office. Accessed July 2006 at: http://www.homeoffice.gov.uk/rds/prgpdfs/fprs112.pdf

Clarke, R. V. (2004). Crime proofing of products: The idea and the substance. *IEEE Technology and Society Magazine*, Fall 2004, 21–27.

Clarke, R. V., & Newman, G. (2005). *Designing out crime from products and systems. Volume 18 of Crime Prevention Studies*. Monsey, NY: Criminal Justice Press.

Cohen, L. E. & Marcus Felson. (1979). Social change and crime rate trends: a routine activities approach. *American Sociological Review, 44,* 588–608.

Cho, Dal-ho, Kang Ryoung Park, Dae Woong Rhee, Yanggon Kim, Jonghoon Yang, "Pupil and Iris Localization for Iris Recognition in Mobile Phones," snpd-sawn, pp. 197–201, Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'06), 2006. Accessed July 2006, at http://csdl2.computer.org/persagen/

Samsung Exhibit 1023, Page 20 of 22

DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/snpd-sawn/2006/2611/00/2611toc.xml&DOI=10.1109/SNPD-SAWN.2006.58
Economist, The (2005). In the very near future. The Economist, 8th December 2005.
Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk, Security and Crime Prevention, 2*, 249–265.
Ekblom, P. (2005). Designing products against crime. In N. Tilley (Ed.), *Handbook of crime prevention and community safety.* Cullompton, Devon: Willan Publising.
Everson, S., & Pease, K. (2001). Crime against the same person and place: Detection opportunity and offender targeting. In G. Farrell & K. Pease (Eds.), *Repeat victimization*. New York: Criminal Justice Press.
Farrell, G. (1997). Skunks, cinnabar moths and smart policing. *Police and government security technology.* 62–63. Croydon: Ballentine Ross. April.
FindYourChild (Undated). FindYourChild. Accessed July 2006 at http://www.findyourchild.net
FollowUs (Undated). FollowUs track a mobile phone. Accessed July 2006 at http://www.followus.co.uk
Gamman, L., & Hughes, B. (2003). Thinking thief: Designing out misuse; abuse and criminal aesthetics. *Ingenia Journal*, 35–42, February.
Geoghegan, T. (2005). 'The password for your next phone is' BBC News online, Accessed 09 June 2005, at http://news.bbc.co.uk/1/hi/magazine/4073208.stm (accessed July 2006).
GSMArena (Undated) Pantech GI100. Accessed July 2006 at http://www.gsmarena.com/pantech_gi100–806.php
Harrington, V., & Mayhew, P. (2001). Mobile Phone Theft. Home Office Research Study 235. London: Home Office. (available at: http://www.homeoffice.gov.uk/rds/pdfs/hors235.pdf).
Karrysafe (Undated). Karrysafe. Accessed July 2006 at http://www.karrysafe.com/home.html
Katz, L. (2006). Brush-on microdots tag your valuables. CNET News.com, 24 February 2006. Accessed July 2006 at http://news.com.com/2061–10801_3–6043209.html
Laycock, G. L. (1985). Property Marking: A Deterrent to Domestic Burglary? Crime Prevention Unit paper 3. London: Home Office. Available at http://www.homeoffice.gov.uk/rds/prgpdfs/fcpu3.pdf
Laycock, G. (2004). The UK car theft index: An example of government leverage. In: M. G. Maxfield & R. V. Clarke (Eds.), *Understanding and preventing car theft,* volume 17 of *Crime prevention studies* (pp. 25–44). Monsey, NY: Criminal Justice Press.
Lester, A. (2001). *Crime reduction through product design. Australian institute of criminology trends and issues # 206*. Canberra: Australian Institute of Criminology.
Mailley, J., Whitehead, S., & Farrell G. (2006a). 'Progress and prospects in the prevention of mobile phone theft'. *Justice of the Peace, 170*(22), 404–407.
Mailley, J., Whitehead, S., & Farrell, G. (2006b). Bring on the safety razr: The top-10 stolen mobile phones. *Justice of the Peace, 170*(30), 564–566.
Mailley, J., Garcia, R., Whitehead, S., & Farrell, G. forthcoming. 'Phone theft index' accepted and forthcoming in Security Journal
Mantyrjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S., & Ailisto, H. (2005). 'Identifying users of portable devices from gait pattern with accelerometers' Oulu, Finland: VTT Electronics. http://virtual.vtt.fi/inf/julkaisut/muut/2005/ICASSP05.pdf
MapAMobile. (Undated). Mapamobile... for your peace of mind. Accessed July 2006 at http://www.mapamobile.com/index.php
Maxfield, M., & Clarke, R. V. (2004). *Understanding and preventing car theft. Volume 17 of Crime Prevention Studies*. Monsey, NY: Criminal Justice Press.
Maxim, (2006). iButton-touch the future. Accessed July 2006 at http://www.maxim-ic.com/products/ibutton
Omron. (2005). Omron Announces "OKAO Vision Face Recognition Sensor", World's First Face Recognition Technology for Mobile Phones. Omron Press Release, 28th February 2005. Accessed July 2006 at http://www.omron.com/news/n_280205.html
Selectamark. Undated. 'Selectamark' (website) Accessed July 2006 at http://www.selectamark.co.uk/product_chelseaclip.html
Sheffield Hallam University (Undated-a). Entry 139: Michael Cross: Chargelock reducing theft and illegal use of mobile phones. Accessed July 2006 at http://www.shu.ac.uk/schools/cs/cri/adrc/dac/p.charge.html
Sheffield Hallam University (Undated-b). entry 136: Luke Worrall-INCharge - reducing theft and illegal use of mobile phones. Accessed July 2006 at http://www.shu.ac.uk/schools/cs/cri/adrc/dac/a.incharge.html
Sheffield Hallam University (Undated-c). Entry 145: Billy Greenhalgh - Theft Deterrent Jewellery. Accessed July 2006 at http://www.shu.ac.uk/schools/cs/cri/adrc/dac/p.billy.html
SmartWater (2006). Smartwater. Accessed July 2006 at http://www.smartwater.com

Samsung Exhibit 1023, Page 21 of 22

Smith, C., Bowers, K. J., & Johnson, S. D. (2006). Understanding bag theft within licensed premises in Westminster: Identifying initial steps towards prevention'. *Security Journal, 19*(1), 3–21.

Smith, T. (2005). Mio GPS smart phone exposed. The Register, Thursday 25th August 2005, Accessed July 2006 at http://www.theregister.co.uk/2005/08/25/mio_a701_exposed

Stoptheft (Undated). Technical Information: Stoptheft microdots. Accessed July 2006 at http://www.stoptheft.co.uk/product/page5.htm

System Concepts (2005).

TraceAmobile.com. (Undated). Trace A Mobile.com. aAccessed July 2006 at http://www.traceamobile.co.uk

Trackitback. (2005). Trackitback: What Do You Have To Lose? Accessed July 2006 at http://www.trackitback.co.uk/ http://www.trackitback.co.uk

Walker, A., Kershaw, C., & Nicholas, S. (2006). Crime in England and Wales 2005/6. Home Office Statistical Bulletin 12/06. London: Home Office. At: http://www.homeoffice.gov.uk/rds/pdfs06/hosb1206.pdf).

View publication stats