RESEARCH

Open Access

Preventing phone theft and robbery: the need for government action and international coordination

Graham Farrell

Abstract

The banning of stolen handsets from networks has been around for 20 years, but remains little used internationally. Where used, its effectiveness is hindered by implementation problems, reprogramming, easy fencing opportunities, and international trafficking. Kill-switches where the user remotely disables a handset and deletes data have potential but, if non-permanent, are likely to experience similar limitations. This study proposes a set of responses to be adopted by national governments with international coordination.

Keywords: Phone theft; Phone robbery; Blacklisting; IMEI database; Kill switch; Phone theft index; Phone theft ratio

Background

"The subjects approached the victim and started asking about his phone, which he had in his hands. Subject 1 then attempted to snatch the phone from the victim. After failing to obtain the phone, subject 1 slashed the victim on his neck with a black utility knife." (crime report from Ryerson University 2014)

"'Robbery victim killed for iPhone' A robbery victim died after he was stabbed in the head with a screwdriver..." (Daily Express 2011)

"The Dutch Ministry of Foreign Affairs confirmed the death ... Kuipers was on her way home with colleagues on Friday in the port city of Tema when their car was surrounded by four armed men on motorcycles. They were robbed of mobile phones, cameras and personal effects." (GhanaWeb 2013)

"In 2013, 3.1 million people reported their smartphones stolen, up from 1.6 in 2012. More people are misplacing their smartphones, too; last year, 1.4 million Americans lost their smartphones, up from 1.2 million in 2012." (Lowe 2014 reporting information from Consumer Reports 2014)

"The Crime Survey [for England and Wales] data begins to give an insight into the variation in crime by demographic factors and suggests that 14–24 year olds, and particularly women, are most vulnerable to mobile phone theft" (Behavioural Insights Team, 2014b; 10)

"mobile device theft costs consumers \$30,000,000,000 [\$30 Billion] each year according to the Federal Communications Commission" (H.R. 4065 House of Representatives, 13th Congress 2014).

As these quotes suggest, the impact of phone theft and robbery upon society is widespread, and the cost is enormous and ongoing. The \$30 billion annual estimate for the United States alone is readily believable when one considers that such costs can include not just that of replacing handsets but also those of the loss of personal and financial data, repairs to cars and households where break-ins occur, medical and health services costs, the emotional and other psychological health costs of victimization and injury to victims and their families, and the cost to society from lost productivity, insurance ad-

Correspondence: graham_farrell@sfu.ca Simon Fraser University, Burnaby, British, Columbia V5A 1S6, Canada



© 2015 Farrell; licensee Springer. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited. ministration costs, policing and the criminal justice system (Mailley et al. 2008).

While the cost of phone theft provides the backdrop, the focus of this study is crime prevention. It is aimed at an international audience of government policy-makers and senior police. However, its coverage cannot aspire to be exhaustive, due to the rapidly evolving technologies and the dynamic market for phones plus significant variation in policy and practice across countries. If it adds value by bringing strands of the topic together and thereby prompts others to pursue some of the issues further, then it will have achieved its goal. It concludes by summarising the problems and potential solutions identified, and these might be easily adapted into a checklist for government and police.

For brevity, the term 'phone theft' is used here as a portmanteau term for crimes where a handset is taken illegally, which can include robberies, burglaries, car break-ins, and various types of theft. Convergence means the overlap between many new technologies is increasingly blurred. Roman and Chalfin (2007) offer the term 'iCrime' to refer to crime relating to smartphones, tablets, laptops, and similar electronic goods that are frequent targets. Hence many of the issues addressed here will likely be relevant to the prevention of other iCrimes.

Method

This study collates and assesses previous research on phone theft and robbery. It incorporates information gleaned from the publications of the phone industry and uses media sources for some more recent information and examples. It draws disproportionately upon the UK experience because of the relatively more extensive information available for that country.

Reliable data on phone theft is relatively scarce. The United Kingdom is an exception, where phone theft drew the attention of that country's government crime research outfit in the 1990s. Harrington and Mayhew's (2001) landmark study showed rapid increases in phone theft, and a set of questions on phone theft was added to the British Crime Survey (now the Crime Survey for England and Wales) in 2001/2 (Hoare 2007; Hall 2009). This work was influential in the decision to establish the Metropolitan Police's National Mobile Phone Crime Unit (NMPCU) in 2003, and to introduce the Mobile Phone Reprogramming Act of 2002 which banned hand-set reprogramming (discussed later).

Increases in phone theft in the last two decades go against the grain of declining crime of many types. Thompson (2014a, 2014b, 2014c) finds that theft and robbery rates have fallen less than many types of crime because they are composed of two underlying trends: "one which mirrors the more general decreases in crime, and one which reflects increased theft due to the greater availability of new, valuable goods that are attractive to thieves and carried on the person, particularly mobile phones." (Thompson, 2014a)

While phone theft has been problematic since the 1990s, it has become increasingly newsworthy with the rise of expensive smartphones (e.g. Choules 2012; Huf-fington Post 2013). In mid-2013, an iPhone 5 with 64GB memory, then top of the range, retailed for over \$1500 in North America at a popular online retailer^a. One experienced police colleague (who shall remain anonymous) conjectured that stealing two handsets per day is easier and more profitable than dealing drugs.

The principal theoretical and conceptual reference points for this study are as follows. Phone theft is an instance of crime caused by an increase in suitable targets offering crime opportunities that attract and provoke offenders (Wortley 2001; Clarke 2012). Hence the present study falls within the crime science tradition, encompassing the routine activity and rational choice theoretical perspectives. Within this, situational crime prevention identifies the mechanisms of victim precaution by which crime is made riskier, more difficult, less rewarding, less excusable, or less provoked, such that quasi-rational offenders decide not to commit crime (Cornish and Clarke 2003). Each of these is critical to the growing literature on designing-out crime and the crime proofing of everyday products (see e.g. Ekblom 2011, 2012).

Results

Anti-theft measures

Some anti-phone-theft measures have been reviewed elsewhere though they have not, to the present author's knowledge, been evaluated in terms of crime prevention impact (Mailley et al. 2006a; Whitehead et al., 2008). They include efforts to secure handsets to the person via clips and lanyard chains, to design more secure bags, and to secure bags in theft-prone locations such as cafes and bars (Arts and Humanities Research Council undated; see Johnson et al. 2010 for responses specific to different types of theft of property from customers in those locations). Policing tactics include raids on stores selling stolen phones and measures to tackle relevant organised criminal groups. The potential deterrent effects of handset iconography and semantics, biometric safeguards (more recently introduced as fingerprint scans on some phone models) and other design features have received some attention (McCardle et al. 2011). However, the principal preventive activity in recent years has been 'blacklisting', and it sets the context for much of what follows.

Blacklisting

In a similar way to how motor vehicles have a unique serial number termed the VIN (Vehicle Identification Number), every phone handset has a unique 15-digit serial number termed the IMEI number - the International Mobile Equipment Identity. When a handset is powered-up it uses the IMEI number to login to the network, in addition to logging in the SIM (Subscriber Identity Module) card. The SIM card identification determines who receives the bill for network charges, and is separate from the handset's IMEI identification - hence SIM cards can be switched from one handset to another with both SIM and handsets retaining their separate identities. Thus, in theory, when a handset is reported stolen two things occur: the network provider will block the SIM card so that the subscriber does not receive further network charges (regardless of which handset is used with that SIM card), and the stolen handset's IMEI number is added to a list of those not allowed access to the network: the blacklist. With the handset being the main target, blacklisting is the focus here.

A stolen phone could, of course, be used on a different network. Hence national and international coordination of blacklisting is necessary. This is intended to work as follows. Nationally for any given country, once all network providers are signed-up to undertake blacklisting, they share their blacklists each day on a national Equipment Identity Register (EIR). Each national EIR is then shared internationally via the international IMEI Database. The international IMEI Database^b and the national EIRs merge the blacklists and return complete lists to all individual network providers, so that everyone can blacklist all stolen phones. Thus, in theory, this should remove the incentive for phone theft because a stolen phone will not work anywhere. A recent industry report noted that

"Every day since 1996, the IMEI Database has taken all the black lists from different operators around the world and added them together into one global black list. When an EIR subsequently connects to the IMEI Database, it downloads the latest global black list (or a national or regional subset of the global list) for its own use. By loading the IMEI Database black list onto the local EIR, all handsets reported as stolen on other connected networks up to the previous day are now also blocked on that network." (CWTA Canadian Wireless Telecommunications Association 2012; 4)

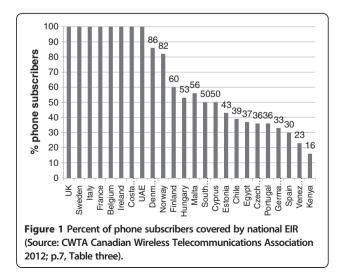
Thus conceived, blacklisting appears to be an elegant means of tackling phone theft. To locate it in the framework of situational crime prevention, blacklisting 'denies the benefits' of crime. What is apparent, however, is that there is a gap between theory and practice. The statement above suggests international blacklisting has existed for two decades - yet phone theft continues apace. Something is amiss. The next few paragraphs outline likely explanations.

Implementation issues

Implementation is a frequent stumbling block for crime prevention (Laycock and Tilley 1995). Most obvious in relation to blacklisting is that although the international IMEI database has existed for twenty years, the number of countries using it remains small. The Canadian Telecommunications and Wireless Association (CWTA, 2012) reports that eight countries had all network providers connected to the international IMEI database and were sharing their blacklists on a daily basis, and that a further 16 countries had some networks connected (Figure 1).

Since the CWTA report, Canada and the United States adopted blacklisting in 2013 (Duncan 2012; Hollister 2013; Canadian Broadcasting Corportation 2013). Yet blacklisting's international coverage remains limited, and the countries that are identified by CWTA (2012) as the main destination countries for trafficked handsets, have little or no blacklisting.

Failure to report crime to the police is a perennial problem. Burglary and car crime are reported more than other crimes when that is a prerequisite of an insurance claim. However there is little incentive for uninsured phone theft victims to report the crime to the police. Here there is what Economists term a public goods problem: the benefit to society that potentially accrues from reporting (due to handset blacklisting) is greater than that to the victim. For victims with insurance, insurers could perhaps incentivise blacklisting along with reporting to the police. This might have the added benefit of reducing false insurance claims that occur when a



handset owner wishes to avoid paying for a handset upgrade. Perhaps insurance premiums could be lower for phone owners who inform the insurer of their handset IMEI, as they are for some cars locked in garages and households with approved security.

The extent to which networks fail to blacklist phones when their theft is reported, is currently unknown. Research using a secret-shopper approach could assess its extent, and publication of the findings would similarly incentivise police and networks to reduce the problem. To tackle the problem, in the UK a Crime Reduction Charter was signed in August 2006 wherein all of that country's network providers agreed to two conditions^c. Network providers agreed to blacklist at least 80 percent of stolen handsets and to share the blacklist across networks within 48 hours. The phone industry conducted its own evaluation under the auspices of the Mobile Industry Crime Action Forum (MICAF) and claims success (Cooper et al., 2007, Mobile Industry Crime Action Forum 2007). While this appears laudable, an independent evaluation with a transparent methodology would be preferable. In addition, if the performance (blacklisting rates) of network providers were a matter of public record, this might induce improved performance as they compete for informed customers. In addition, the commitment should be to blacklist 100 percent of stolen handsets.

Reprogramming

Reprogramming trumps blacklisting. It is an adaptive response by offenders (Ekblom 1997) to blacklisting as a form of crime prevention. Stolen handsets, like stolen cars, can have their identity changed in order that they can re-enter the legal market. Typically, the handset software is reprogrammed to change the IMEI to one that is valid on the network. While this has been illegal in the UK since 2002, from the evidence relating to the scarcity of blacklisting, it is reasonable to infer that it remains legal in most other countries. One study estimated that at least 5 percent and perhaps 8 percent of phones in use in the UK were reprogrammed (Kaplankiran et al. 2008), implying millions of stolen phones in circulation, which seems likely to be a conservative estimate. Rates of stolen phones in circulation can reasonably be expected to be higher in countries where reprogramming is legal.

Reprogramming of some phones has become trickier where the IMEI is stored on a non-reprogrammable chip. Some smartphones have an internal nonremovable battery and the shell is more difficult to open. It takes greater expertise to physically replace a chip rather than alter software. However, there are webpages offering instructions on how to change, for example, the IMEI of some iPhone models,^d and many smartphone models are reprogrammable (Lynn and Davey 2014).

A reprogrammed phone uses an IMEI number that is a *duplicate* of that of a legitimate phone in order to be able to login to the network when its original IMEI is blacklisted (Kaplankiran et al. 2008). This means that if duplicate IMEIs can be identified then they can be blacklisted. Mailley et al. (2006a) note that Vodafone Ireland successfully identified duplicate IMEIs and blacklisted them in order to stop stolen phones from working. Since networks can identify and blacklist duplicate IMEIs, this offers a relatively straightforward solution to the problem. If there are legitimate reasons why a duplicate IMEI is needed, those phones should be easily identifiable. If this practice was widespread and routinized, it could have a dramatic effect by disabling stolen phones on any network that shares that blacklist. In addition, it seems likely that customers who had turned a blind eye to the fact that their bargain handset was probably stolen would be less inclined to make the same mistake again if it failed to make calls.

The kill-switch

Proposed 'kill switches' would be activated remotely by phone owners whose handset had been stolen. This would trigger deletion of handset data and disable all handset operations. This appears to have the advantage of being more comprehensive and possibly more difficult to overcome than blacklisting. Legislative efforts to mandate kill switches in the United States, ongoing at the time of writing, require that phones can be reactivated if recovered (Consumer Reports 2014). This suggests kill-switches would temporarily disable handsets rather than permanently 'kill' them, which in turn suggests there may be some potential for reprogramming of the software to circumvent the kill-switch. Similarly, while remote data deletion ought to reduce the chances of additional financial or personal damage to the victim, to the author's knowledge, the potential for hacking to circumvent data deletion remains unknown at the time of writing.

While this discussion of kill-switches comprises a relatively small section of the present study, they are a potentially significant intervention (Collins 2014). However, if kill-switches experience implementation problems and reprogramming (and other hacking) as blacklisting has their potential may be unachieved. By introducing this discussion of kill-switches here, it would be hoped that some or all of the problems could be anticipated and resolved prior to widespread implementation. The spectre of reprogramming suggests that government should seek to liaise with the phone industry to anticipate and overcome such possibilities.

Phone recycling

'Recycling' is largely synonymous with ethical practices, but in this context it is criminogenic. For example, as of mid-2014 one Canadian firm posted online prices for smartphones, iPads and other tablets that it would buy from customers who send them by mail (CellCycle.ca 2014a). It listed prices for 256 make/model combinations with prices over \$200 for many smartphones and upto \$400 for tablets (CellCycle.ca 2014b). Its online notices state that "All Apple product MUST have iCloud accounts removed and 'Find My iPhone' disabled to qualify for payment", which reduces the possibility of identification of stolen items. The Terms of Purchase say that "We do not retain [the sellers] information for any purpose other than making payment to you." (CellCycle. ca 2014c), and that "You must warrant that you are: the owner of the device(s) that you wish to sell us" and that the phone "must not be identified on any database as lost or stolen", although there appears to be no means by which these claims are verified. This appears to be an easy way for thieves to sell stolen phones with impunity. It seems likely to encourage theft and robbery. Yet at the time of writing such companies have been operating in Canada since 2007 (Canadian Broadcasting Corporation 2009) which, perhaps not coincidentally, is the year the iPhone was released.

In the UK, recycling firms pay similar prices (BBC 2010a). In 2010, fifteen UK recycling firms, suggested to represent 90 percent of the industry, signed up to a code wherein they check the IMEIs of handsets against the National Mobile Phone Register which is a national database of stolen phone IMEIs (BBC 2010a). While this would appear to be a policy worthy of replication elsewhere, it would be unlikely to be effective without enforcement, and there do not appear to be plans to make available information on monitoring or evaluation of adherence to the code. It would be informative to know if the code had reduced the likelihood that a recycling company turns down a valuable new smartphone, and naïve not to expect firms or employees to turn a blind eye to handsets which sell for even more money abroad than in the UK. If firms were publicly accountable, this would increase any deterrent effect. Again, a secretshopper monitoring or detection and enforcement system, offering blacklisted smartphones to recycling firms and publicised to maximise its deterrence effect, could promote adherence, particularly if poorly operated firms can be closed-down (just as unhealthy restaurants are closed). Some consideration might be given to safeguards to ensure that the employees of recycling firms do not divert stolen phones to alternate fences. In addition, recall that even the industry only claimed a 90 percent sign-up to the charter. A police investigation that examined whether the remaining 10 percent are disproportionately receiving stolen phones (or whether phone theft rates are higher in neighbourhoods nearest to unchartered recyclers) might be useful, as would requiring their sign-up and adherence to the Charter.

Other aspects of the stolen goods market

When a store in Detroit bought electronic goods over the counter, no questions asked, customers lined up along the street. The store had no identity check requirements for sellers, or checks on the provenance of goods. It was, in effect, licensed fencing, with customers bringing sometimes dozens of phones, laptops and tablet computers (Smith 2013). Such practice can be expected to facilitate, prompt and provoke theft and robbery, and similar accusations could likely be levelled at eBay, Craigslist and other online resellers. There is a clear need for harmonisation of regulation relating to such practices.

An array of measures have been proposed to tackle stolen goods markets (Sutton 2005). In the case of phones, measures might be tailored to particular modes of sale and local circumstances. One design possibility is a 'licence plate'. Displaying a handset's identity on its exterior could nudge buyers and sellers into a greater proportion of legal activity. Portable phones have long carried an IMEI label, typically hidden under the battery in tiny print. If IMEI numbers were routinely made visible on the exterior of handsets this would allow potential buyers to check whether it matched the IMEI in the phone's software. Typing *#06# onto the touchpad of most phones reveals the 15-digit IMEI number. The overall effect would be to raise the profile of the theft problem and shrink the stolen handset market via at least five mechanisms: Buyers of pre-owned handsets could check that handset and software IMEIs match and are not on the blacklist; Retailers could no longer claim ignorance regarding stolen or reprogrammed phones; Online sellers would soon be obliged to state that they have verified a handset IMEI; Police could more easily check whether a handset is stolen, and; The visibility of IMEIs would promote the transfer of information for blacklisting.

The phone licence plate is a concept that draws on vehicular security. Licences facilitate identification of otherwise identical individual units. Vehicle owners were first required to display their name on their vehicle, then in 1903 the state of Massachusetts introduced licence plates (Newman, 2004). For phones, design effort would be required to identify suitable licence plate parameters and make them attack resistant. A system with less than 15 digits (vehicle plates typically uses seven alphanumeric) would make them more memorable thus also promoting reporting and recording for blacklisting purposes.

International trafficking

Phones blacklisted in one country will still work in all but ten others according to the above assessment of use of the international IMEI database. The average price of a handset may be higher in other countries than in the 'source' country where it is stolen, making trafficking worthwhile: in 2013, smartphones stolen in the UK were reported to sell for up to £1,000 in other countries (Telegraph, The 2013). The present study has identified only one effort to measure the extent of trafficking, detailed in Mailley et al. (2006a), and suggesting that handsets stolen in the UK turned up in countries around the world. That research was conducted by the O2 network provider and consisted of providing networks in other countries with a copy of the UK handset blacklist and asking them to identify any calls made on their networks from those handsets. The same work, now rather dated, appears to be the source of the Canadian Wireless Telecommunications Association (CWTA Canadian Wireless Telecommunications Association 2012; 3) report that notes stolen handsets account for 90% of handsets sold in Russia, 85% in the Ukraine, 66% in Central and Eastern Europe, and 27% in Africa and the Middle East. One presumes data on Western Europe and north America was less readily available or unsought. Such research warrants replication and extension. It could potentially be used to identify key countries and trafficking relationships and thereby used to focus prevention activities.

A note of caution is necessary, however, due to the paucity of information on trafficking because, with regard to the international trafficking of cars from the UK, Clarke and Brown (2003) found it was far *less* extensive than many commentators had anticipated. However, while the precise extent, nature and variation in trafficking warrants further study, this should not preclude some discussion of prevention possibilities.

The international IMEI Database is a potential key to reducing international trafficking. It was described earlier and requires the daily exchange of network blacklists on an international basis, and its main problem for two decades has been lack of coverage. However, it may be possible to incentivise manufacturers and networks to stem the sale of imported stolen phones. In particular, manufacturers in recipient countries seem to effectively lose market share if phones stolen elsewhere are sold in their market: Mailley et al. (2006a; 406) report that a survey of customers in Russia found Motorola to be the most popular make of handset even though Motorola did not sell handsets in that country (at a time when the Motorola Razr not the iPhone was the iconic handset). An estimate of their losses might encourage manufacturers in domestic markets to reduce the number of imported stolen phones. The manufacturers might have the leverage to encourage network providers to use the international IMEI Database. The industry could perhaps argue that the international IMEI Database is difficult to use, which seems an untenable argument from such a technically sophisticated industry, particularly due to its existing use elsewhere.

Regulation and market-based incentives

It is fairly well established that industry is best placed to develop anti-crime measures relating to its own products and services (Clarke and Newman 2005). This is because the relevant industry has the technical know-how and inside knowledge. The flagship case is the car industry. Car theft increased rapidly during the 1960s, 70s and 80s but has been stemmed by vastly improved vehicle security, with remote tracking technologies offering promise of continuing declines (Brown, 2004, Flatley et al. 2010, Fujita and Maxfield 2012, van Ours and Vollaard 2013 Farrell et al. 2014). Yet car manufacturers took time to introduce such measures and often had to be pushed into it by the public shaming of a wellpublicised car theft index, or forced into it via regulation (Laycock 2004). The differential timing of the introduction of good quality electronic immobilizers in different countries suggests that national legislation or threat of such tended to play a key role.

There is also evidence that when crime affects the phone industry itself, it responds efficiently and effectively. Fraudulent calls using phone 'clones' that cost the industry millions were stopped in their tracks (Clarke et al. 2001). When it comes to theft of handsets however, there may be perverse incentives for the industry to turn a blind eye: A stolen phone generates a new sale for manufacturers when the handset is replaced, while network providers generate call revenue from both the stolen and the new phones. But even if this is not the case, there seems to be little incentive for the industry to act, as it would inevitably incur costs. It is cheaper for the phone industry to allow victims and society to continue to pay the cost. This suggests there is an important role for government in overcoming this failure of the market.

Theft indices

Theft indices are a form of market-based incentive for crime reduction. The UK government announced in 2013 that it would support the development of a phone theft index (Beckford 2013). A risk-based phone theft index was described by Farrell and Mailley (2007) as a development of a simpler count-based index (Mailley et al. 2006b, Mailley et al., 2008), wherein

"The new ranking presented in this article is based on phones' risk of being stolen, taking into account that some phone models sell better and are more likely to be on the streets than others." (Farrell and Mailley, 2007; 30)

Those authors also reported on interviews conducted with phone thieves. Thieves noted how they make decisions to steal some models rather than others based on visual cues about the model of phone and its value:

"Offenders use visual cues to assess whether a phone is worth the effort... for indicators of value and whether or not it will be easy to fence. Thieves obviously prefer the more valuable phones. Just as prestige cars are targeted for 're-sale' thefts, iconic 'in-demand' phones and expensive models with sophisticated functions, are targeted." (Farrell and Mailley, 2007; 30)

It is well established that burglars and car thieves use visual cues to make informed choices about targets (Taylor and Nee 1988; Bichler-Robertson and Potchak 2002; Light et al. 1993; Cromwell and Olsen 2003; Nee and Meenaghan 2006). Similar decision processes mean that snatches, sneak thefts (dipping and ripping into bags) and robberies, are more likely to be precipitated by potentially lucrative smartphone models. In contrast, phones stolen during burglaries and car break-ins would not likely involve prior knowledge of the handset model. The distinction between these two types of theft (choice and non-choice of model type), presented as a ratio, was the basis for identifying the riskiness of different models in the risk-based index (Farrell and Mailley 2007, Mailley 2011).

In the UK, data to generate a routine phone theft index is held by the NMPCU. It is likely that an index can be simply, cheaply and routine produced on a timely basis. The phone handset market is faster moving than that for cars so a quarterly rather than annual index might be appropriate, though at minimum a well publicised annual index should stimulate preventive activity among manufacturers. It seems likely that additional work would be needed to develop similar capacity in other countries.

After the present study was completed and accepted for publication, the UK's Home Office published a riskbased phone theft index using the methodology described above. The report contains a useful review of theft risks in that country and the phone theft ratio shows Apple iPhones 4 and 5 to be riskiest. The provenance of the method is acknowledged in a blog post (Behavioural Insights Team 2014a, 2014b).

Government purchasing power (GPP) is a potentially powerful nudge to use alongside a phone index. If government buyers preferred phone models and networks that perform best on crime prevention indicators such as those discussed here (assuming similar quality of other services), that would most likely encourage security.

Anticipating hurdles

Some commentators have raised the spectre of obstructionism. The term was coined to capture the array of impediments that arise, often seemingly inadvertently, when vested interests are at work. It was recently reported that

"A "kill switch" which would help prevent a smartphone being stolen has been rejected by mobile phone carriers in the United States, with government officials accusing companies of "shaking down" customers for billions of dollars in insurance costs." (Johnson 2013).

It seems likely that the phone industry, comprising handset manufacturers and network providers, will raise objections to the development of implementation of measures that incur costs, even if there is a greater net benefit to the rest of society. Three potential areas where this issue could arise are outlined here by means of example: First, the prevention efforts are not technically feasible; Second, they are too costly; Third, the crime will only displace and so there is no point.

Objections relating to technical feasibility are probably the trickiest to overcome because there are few people outside of the phone industry with the same detailed know-how of the hardware, software and systems. This means that discussions of such technicalities could quickly deteriorate, with the well-meaning police officer or policy wonk quickly overwhelmed. Advanced planning would be the best means of overcoming this, as well as using specialised knowledge where it exists. In the UK, for example, this might be lodged at the NMPCU, though since this national police unit has received funding from the phone industry, there could conceivably be competing interests.

Objections relating to cost were once the industry's objection to blacklisting, along the lines of 'Thirty seconds per call operator, at so-many calls per day over a year costs us the equivalent of n millions of pounds'. Such objections should, with some preparation, be tackled with evidence of how small the cost is in the relative picture of overall industry costs as well as the far greater cost to society of the crimes involved. Promoting corporate social responsibility offers a potential terminology here.

Objections relating to displacement should, in theory, be most easily overcome due to the broad range of evidence and arguments against it. The comprehensive review of evidence by Guerette and Bowers (2009) finds that, in short, most good crime prevention efforts produce little or no displacement and many often produce the opposite - a 'diffusion of benefits' wherein crime also falls in unanticipated ways or places as a result of the intervention.

Anticipating future crimes

A means of side-stepping industry reluctance might be to anticipate new criminogenic developments. Whitehead and Farrell (2008), for instance, argued that forthcoming contactless swipe-payments would produce a crime harvest. Subsequently, the UK phone industry's body published a press release noting a range of preventive activities, particularly PIN-code requirements for any non-trivial payments, and automated detection of multiple rapid payments (a signature of possible theft) and 'encouraging' contactless payment customers to sign-up to ensure their IMEI numbers are registered (Mobile Industry Crime Action Forum 2009). One additional way of promoting industry action might be to educate the industry's chief executives with respect to the experience of some of the robbery victims who received serious injuries.

Continued crime-proofing should be a part of any crime reduction efforts. Interviews with phone thieves suggest biometric locks and proximity alarms would induce a deterrent effect (McCardle et al. 2011), though the iPhone 5's 'Touch ID' fingerprint scanner and similar technologies do not seem to have been formally evaluated^e. In addition to proposed kill-switches and remote deletion of data, software that facilitates tracking of handsets without requiring the cooperation of phone networks, may increase detection possibilities, though currently these are overcome simply by powering-off the device. Likewise, phones can increasingly synchronise and interact with other electronic products. One of these allows a phone user to connect to their car, to view inside it, lock it, start the engine, and to track and potentially disable the vehicle if stolen (BBC 2010b). Such measures appear laudable but should be subject to crime proofing, that is, the system should be checked to ensure it does not provide additional crime opportunities. In this instance, if a phone is stolen, its connectivity might increase the chance that the car to which it is paired is also stolen. Hence, as phones become increasingly integrated with household, business and other security, there is a need for crime-proofing to ensure such own-goals do not result.

Conclusion

The enormous success of the car industry in preventing theft of its products is arguably the flagship for promoting the involvement of industry in security and crime prevention. Better vehicle security means car theft has fallen, often by around three-quarters, in many advanced countries (Farrell et al. 2011). This provides clear evidence that a seemingly intractable high volume crime can be prevented by improved design, without much if any displacement. However, while it provides further evidence that industry is best placed to develop product security, it also shows the need to overcome market failure via a mix of regulation and incentives. There is growing evidence that market failure is common when it comes to crime prevention, because there is no natural incentive for the relevant industry to develop the required security. If left to its own devices, no industry will pay for security without an added incentive to do so. This necessitates government intervention, and it took many years to incentivise car security. There is a clear case for more immediate and more forceful action by government to promote efforts to curtail phone theft, and for international coordination to plug the gaping holes in use of the international IMEI database. The alternative is an apathy that effectively causes more crime at great cost to victims and society.

The core activity to prevent phone theft to date has been the blacklisting of phone handsets. An examination of blacklisting and its sequalae was central to the present study. A number of problems with blacklisting and other areas were identified and these are summarised in Table 1 along with the solutions proposed herein. In some ways this is a shopping list of measures that could potentially be used as a springboard for action by governments. The available evidence suggests that the UK has gone some way to introducing some of the measures but that most countries remain largely in the starting blocks.

Many of the issues detailed here in relation to blacklisting seem likely to be relevant to more recently proposed 'kill-switches'. While kill-switches could conceivably have a higher implementation rate if they are triggered by users, there appears to be a need for government and industry to anticipate potential software hacking that would circumvent the kill-switch. Key areas identified where action by national governments is often likely to be required are the lack of coverage and implementation of blacklisting, the possibility of reprogramming, 'recycling' and other forms of criminogenic resale markets, and international trafficking.

The set of measures recommended here will require political will and for technical expertise to be developed by police, governments, and international agencies. In the dynamic phone market where technology and crime opportunities evolve rapidly, promoting the responses identified here should be viewed as a starting point.

The harmonisation of best practice, encouraged via an international body, would seem to be one possible way forward. An international convention or charter would

Table 1 Problems and solutions

Page 9 of 11

Problem	Proposed solution
A. Lack of coverage	
International IMEI database unused	Concept: International bodies and agencies promote national-level blacklisting
	How: Governments encourage national networks. United Nations promotes international treaty obligations. Monitoring and publicity.
National EIR unused or partially used	Concept: Promote blacklisting by networks.
	<i>How:</i> Incentives and regulation by government, monitoring and enforcement of adherence.
B. Stolen phones remain unblacklisted	
Theft unreported to network.	Concept: Encourage reporting.
	<i>How:</i> Incentivise victim reporting via insurers; Require police communication to phone networks; Regulate networks and incentivise call takers to solicit information from callers.
Theft reported but IMEI unknown to victim.	Concept: Networks can identify IMEIs.
	How: Regulate networks; Networks incentivise call takers to identify IMEIs and blacklist them.
IMEI not blacklisted by network.	Concept: Require blacklisting.
	How: Regulate networks to require blacklisting; Phone theft index; Monitoring (e.g. secret shopper surveys), publicity and fines.
C. Reprogramming	
Handset reprogramming	Make reprogramming illegal. Incentivise design-solutions by phone industry. Po- licing tactics.
Duplicate IMEIs allow stolen phones to work	Networks should blacklist duplicate IMEIs.
D. Kill-switches	
Kill-switches potentially vulnerable to reprogramming and other hacking	Requires government to liaise with industry to anticipate and design-out problem
E. Stolen goods markets	
Recycling: Stolen handsets bought by recycling firms	Regulation of recycling firms; Monitoring with publicity; Enforcement with fines.
High street and online secondhand goods markets	Regulation; codes of conduct; transparency and accountability of buyers and sellers.
F. Handset trafficking	
Stolen handsets shipped to markets without blacklisting	International promotion of blacklisting; Monitoring and enforcement of use of international IMEI Database. Market research to identify and target destination markets and networks.
	Manufacturers (who lose market share) should be informed of market share lost to trafficking.
G. Future developments	
New technologies, offender adaptations and other change may	Anticipatory crime-proofing.

New technologies, offender adaptations and other change may Anticipatory crimeproduce new incentives for theft and robbery

require buy-in from governments, and would allow those with little knowledge of the technology to avail themselves of the expertise of others. Best practice guidelines for national governments in relation to each of the areas addressed here would seem to be a minimal requirement and could be relatively easily compiled. The United Nations Office on Drugs and Crime (UNODC) might be an appropriate agency to encourage adoption of the international IMEI Database. Perhaps an International Convention on Traffic in Telecommunications Products, or an additional protocol to the 1973 International Telecommunication Convention, could require IMEI database sign-up, blacklisting charters, reprogramming illegality and other measures by member states. CITES (the Convention on International Trade in Endangered Species) or the 1961 Single Convention on Narcotic Drugs provide potential models for frameworks against trafficking, and the International Narcotics Control Board a possible template for a monitoring agency.

Endnotes

^aTwo retailers listed the 64GB Apple iPhone 5 at this price or over on Amazon on 26 July 2013.

^bGSMA IMEI database at http://www.gsma.com/technicalprojects/fraud-security/imei-database accessed 24 April 2014.

^cA copy of the Mobile Phone Industry Crime Reduction Charter is at http://www.micaf.co.uk/uploads/micaf.pdf accessed 24 April 2014.

^dFor example, see iClarified's 'How to change your IPhone IMEI with ZiPhone' at http://www.iclarified.com/ entry/comments.php?enid=657#commentsanchor accessed 13 July 2011.

^eThe Apple iPhone 5 was the latest model from that manufacturer at the time of writing.

Competing interests

The author declares that he does not have any competing interests.

Received: 25 July 2014 Accepted: 21 December 2014 Published online: 04 March 2015

References

- Arts and Humanities Research Council. (undated). Fighting Crime through More Effective Design. At http://www.ahrc.ac.uk/News-and-Events/Publications/ Publications-archive/Documents/General/Fighting-crime-through-effectivedesign.pdf accessed 07 March 2013.
- BBC (2010a), 'Stolen mobiles strategy agreed by phone recycling firms', *BBC News* online, 23 July 2010, at http://www.bbc.co.uk/news/uk-10724805.
- BBC (2010b), 'The phone that could stop car theft', *BBC News Online*, 15 October 2010, at http://news.bbc.co.uk/1/hi/programmes/click_online/9095459.stm.
- Beckford, M. (2013). Is your phone the one most likely to be stolen? Downing Street to publish 'risk index' of handsets to encourage shoppers to buy safer models. The Daily Mail, 22 July 2013, at http://www.dailymail.co.uk/news/article-2371797/Downing-Street-publish-risk-index-phones-advise-safer-models.html accessed 23 July 2013.
- Behavioural Insights Team. (2014a). Empowering consumers in order to reduce mobile phone theft. at http://behaviouralinsights.co.uk/blogpost/empoweringconsumers-order-reduce-mobile-phone-theft accessed 29 September 2014.
- Behavioural Insights Team. (2014b). *Reducing Mobile Phone Theft and Improving Security*. London: Home Office.
- Bichler-Robertson, G, & Potchak, MC: (2002). Testing the importance of target selection factors associated with commercial burglary using the blended approach'. *Security Journal*, 15, 14–61.
- Brown, R. (2004). The effectiveness of electronic immobilisation: Changing patterns of temporary and permanent vehicle theft'. In M. G. Maxfield & R. V. Clarke (Eds.), Understanding and Preventing Car Theft. Monsey, NY: Criminal Justice Press.
- Canadian Broadcasting Corporation. (2009). 'Cellphone recycling program starts in B.C. [British Columbia]'. 11 November 2009 at http://www.cbc.ca/news/ canada/british-columbia/cellphone-recycling-program-starts-in-b-c-1.805778 accessed 24 April 2014.
- Canadian Broadcasting Corportation. (2013). 'Stolen phones blacklist launches in Canada'. at http://www.cbc.ca/news/technology/stolen-phones-blacklist-launches-in-canada-1.1873674 accessed 01 October 2013.
- CellCycle.ca. (2014a). 'Cash to recycle cell phones in Canada'. website at http:// www.cellcycle.ca/2010/04/12/cash-for-cell-phone-recycling-in-canada/ accessed 24 April 2014.
- CellCycle.ca. (2014b). 'Purchase pricing'. at http://www.cellcycle.ca/pricelist.pdf accessed 24 April 2014.
- CellCycle.ca. (2014c). Wireless device claim form'. at http://www.cellcycle.ca/ claimform.pdf. accessed 24 April 2014.
- Choules, R. (2012). *Mobile phone theft rises by 25pc in three years*'. The Telegraph, 08 Nov 2012. At http://www.telegraph.co.uk/finance/personalfinance/consumertips/9663807/ Mobile-phone-theft-rises-by-25pc-in-three-years.html accessed 19 March 2014.
- Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime Science*, 1(2), 1–9.
- Clarke, RV, & Brown, R. (2003). International Trafficking in Stolen Vehicles'. In T. Michael (Ed.), Crime and Justice, Volume 30 (pp. 197–227). Chicago: University of Chicago Press.

- Clarke, RV, & Newman, G. (2005). Modifying criminogenic products: What role for government?'. In R. V. Clarke & G. Newman (Eds.), *Designing out crime from products and systems*. Monsey, NY: Criminal Justice Press.
- Clarke, RV, Kemper, R, & Wyckoff, L. (2001). Controlling cell phone fraud in the U. S. Security Journal, 14, 7–22.
- Collins, B. (2014). 'iPhone theft falls because of iOS 7 security' PCPro, 08 September 2014, at http://www.pcpro.co.uk/news/390682/iphone-theft-fallsbecause-of-ios-7-security.
- Consumer Reports. (2014). 'Smart phone thefts rose to 3.1 million last year'. 17 April 2014, at http://www.consumerreports.org/cro/news/2014/04/smartphone-thefts-rose-to-3-1-million-last-year/index.htm , accessed 27 April 2014.
- Cooper, C, Ek, A, Heasman, T, & Stewart, T. (2007). *Report for the Mobile Industry Crime Action Forum on Testing the Processes for Blacklisting Mobile Phones Reported as Stolen to the UK Mobile Networks*. London: System Concepts.
- Cornish, DB, & Clarke, RV (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention'. *Crime Prevention Studies*, 16, 41–96.
- Cromwell, P, & Olsen, J. (2003). *Breaking and Entering: Burglars on Burglary*. Belmont CA: Wadsworth.
- CWTA (Canadian Wireless Telecommunications Association). (2012). Comparison of International Handset Security Measures. Ottawa: CWTA. 13 August 2012. At http:// cwta.ca/wordpress/wp-content/uploads/2011/09/Comparison-of-International-Handset-Security-Measures-2012-08-13.pdf accessed September 2013.
- Daily Express. (2011). 'Robbery victim 'killed for iPhone". Express online, 07 February 2011, at http://www.express.co.uk/news/uk/227700/Robbery-victim-killed-foriPhone accessed 02 October 2014.
- Duncan, G (2012). 'How stolen phone blacklists will tamp down on crime and what to do in the mean time' *Digital Trends*, At http://www.digitaltrends. com/mobile/combatting-theft-with-stolen-phone-blacklists/#!bc9mr9. Accessed 13 October 2013.
- 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. (2011). Crime Prevention, Security and Community Safety using the 5/s Framework. New York: Palgrave Macmillan.
- Ekblom, P. (Ed.). (2012). *Design Against Crime: The Crime-Proofing of Everyday Products.* London: Lynne Rienner Publishers.
- Farrell, G and Mailley, J (2007), 'Phone alert: Mobile phone crime is increasing as thieves target the ever more valuable handsets' *Police Review*, 27 July 2007; 30–31.
- Farrell, G, Tilley, N, & Tseloni, A. (2014). Why the crime drop?'. In M. Tonry (Ed.), Why Crime Rates Fall and Why They Don't, volume 43 of Crime and Justice: A Review of Research. Chicago: University of Chicago Press.
- Farrell, G, Tseloni, A, Mailley, J, & Tilley, N. (2011). The crime drop and the security hypothesis'. Journal of Research in Crime and Delinquency, 48(2), 147–175.
- Flatley, J, Kershaw, C, Smith, K, Chaplin, R, & Moon, D. (2010). Crime in England and Wales 2009/10: findings from the British Crime Survey and Police Recorded Crime (Home Office Statistical Bulletin, 12/10). London: Home Office.
- Fujita, S, & Maxfield, M. (2012). Security and the drop in car theft in the United States. In J. J. M. van Dijk, A. Tseloni, & G. Farrell (Eds.), *The International Crime Drop: New Directions in Research* (pp. 231–249). Basingstoke: Palgrave Macmillan.
- GhanaWeb. (2013). 'Dutch woman confirmed dead in Tema robbery'. 11 March 2013, at http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel. php?ID=267290 accessed 02 October 2014.
- Guerette, RT, & Bowers, KJ. (2009). Assessing the Extent of Crime Displacement and Diffusion of Benefits: A Review of Situational Crime Prevention Evaluations. *Criminology*, 47(4), 1331–1368.
- Hall, P. (2009). 'Mobile phone ownership and theft'. In J. Flatley, D. Moon, S. Roe, & S. Moley (Eds.), *Home Security, Mobile Phone Theft and Stolen Goods* (Statistical Bulletin 10/09, pp. 31–50). London: Home Office.
- Harrington, V, & Mayhew, P. (2001). Mobile Phone Theft (Home Office Research Study 235). London: Home Office Development and Statistics Directorate.
- Hoare, J. (2007). 'Mobile phones: Ownership and theft'. In J. Flatley (Ed.), *Mobile Phone Theft, Plastic Card and Identity Fraud: Findings from the 2005/06 British Crime Survey* (Statistical Bulletin 10/07, pp. 9–28). London: Home Office.
- Hollister, S. (2013). 'Stolen smartphone database is complete, says CTIA'. At http:// www.theverge.com/2013/11/27/5153694/stolen-smartphone-database-iscomplete-says-ctia Accessed 14 January 2014.
- HR. 4065 (House of Representatives), 13th Congress. (2014). Smartphone Theft Prevention Act. at http://www.gpo.gov/fdsys/pkg/BlLLS-113hr4065ih/pdf/ BlLLS-113hr4065ih.pdf or https://www.govtrack.us/congress/bills/113/hr4065/ text accessed 27 April 2014.

Huffington Post. (2013). As of 23 April 2014 there were four in-depth reports on phone theft. at http://www.huffingtonpost.com/tag/phone-theft/.

- Johnson, SD, Bowers, KJ, Gamman, L, Mamerow, L, & Warne, A. (2010). Theft of Customers' Personal Property in Cafes and Bars (Problem-Specific Guides series number 60). Washington: D.C. Office of Community Oriented Policing Services.
- Johnson, D. (2013). "Kill switch' to prevent phone theft rejected in US'. The Telegraph, 20 November 2013, at http://www.telegraph.co.uk/technology/mobile-phones/ 10462027/Kill-switch-to-prevent-phone-theft-rejected-in-US.html accessed 14 January 2014.
- Kaplankiran, T, Mailley, J, Whitehead, S, & Farrell, G. (2008). Mobile phone reprogramming: Its extent and prevention'. *Crime Prevention and Community Safety: An International Journal*, 10(4), 271–279.
- 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* (pp. 25–44). Monsey, NY: Criminal Justice Press.
- Laycock, G, & Tilley, N. (1995). Implementing Crime Prevention. Crime and Justice, 19, 535–584.
- Light, R, Nee, C, & Ingham, H. (1993). Car Theft: The Offender's Perspective. Home Office Research Study No. 130. London: HMSO.
- Lowe, L. (2014). 'U.S. smartphone thefts doubled last year: How to protect your phone' Parada. 18 April 2014, at http://parade.condenast.com/281418/ linzlowe/u-s-smartphone-thefts-doubled-last-year-how-to-protect-yourphone/ accessed 27 April 2014.
- Lynn, G, & Davey, E. (2014). Black market; for stolen phones exposed' BBC News online. 14 April 2014.
- Mailley, JC. (2011). The prevention of mobile phone theft: a case study of crime as pollution; rational choices and consumer demand (PhD dissertation). Loughborough: Loughborough University. at https://dspace.lboro.ac.uk/ dspace-jspui/handle/2134/9645.
- McCardle, J, Storer, I, Whitehead, S, Mailley, J, Torrens, G, & Farrell, G. (2011). Offending users: Designing in deterrence with mobile phones'. *The Design Journal*, 14(3), 323–342.
- 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. (2008). Phone theft index. Security Journal, 21(3), 212–227.
- Mobile Industry Crime Action Forum. (2007). 'MICAF publishes annual report on Crime Reduction Charter'. MICAF Press Release, August. At http://www.micaf. co.uk/home.asp?Page_Info=14 downloaded 02 October 2014.
- Mobile Industry Crime Action Forum. (2009). *Taking the initiative in the fight against mobile phone crime'*. Press Release, 28 August, at http://www.micaf.co. uk/home.asp?Page_Info=14 accessed 30 September 2014.
- Nee, C, & Meenaghan, A. (2006). Expert Decision Making in Burglars. British Journal of Criminology, 46(5), 935–949.
- Newman, G. (2004). 'Car Safety and Car Security: An Historical Comparison'. In M. G. Maxfield & R. V. Clarke (Eds.), Understanding and Preventing Car Theft (pp. 217–248). Monsey, NY: Criminal Justice Press.
- Roman, J, & Chalfin, A. (2007). *Is there an iCrime wave?* Washington DC: Urban Institute, Justice Policy Center.
- Ryerson University. (2014). 'Robbery with a Weapon 2014-07-23'. At http://www. ryerson.ca/irm/alerts_reports/alerts/U_21_14_Robbery_with_a_Weapon.html accessed 02 October 2014.
- Smith, G (2013). Inside the massive global black market for smartphones. *Huffington Post*, at http://www.huffingtonpost.com/2013/07/13/smartphoneblack-market_n_3510341.html. accessed January 2014.
- Sutton, M. (2005). 'Complicity, Trading Dynamics and Prevalence in Stolen Goods Markets. In N. Tilley (Ed.), *Handbook of Crime Prevention and Community Safety* (pp. 294–305). Cullompton: Willan.
- Taylor, M, & Nee, C. (1988). The Role of Cues in Simulated Residential Burglary'. British Journal of Criminology, 28, 105–116.
- Telegraph, The. (2013). Stolen smartphones selling for up to £1,000'. The Telegraph, 05 February 2013, at http://www.telegraph.co.uk/technology/mobile-phones/9849471/ Stolen-smartphones-selling-for-up-to-1000.html accessed 27 April 2014.
- Thompson, R. (2014a). 'Cashing in on mobile phones: Goods stolen through theft and robbery since 1993' Unpublished manuscript. Northampton University.
- Thompson, R. (2014b). Understanding theft from the person and robbery of personal property victimisation in England and Wales 1994-2010/11 (PhD Thesis). Nottingham: Nottingham Trent University.

- Thompson, R. (2014c). 'How theft and robbery have changed from the 90s' *Significance*, 21 October, at http://www.statslife.org.uk/social-sciences/1842how-theft-and-robbery-have-changed-since-the-90s.
- van Ours, JC, & Vollaard, B. (2013). The engine immobilizer: A non-starter for car thieves. CESifo Working Paper: Public Choice, No. 4092 (Centre for Economic Studies and Ifo Institute). Munich: University of Munich.
- Whitehead, S, Mailley, J, Storer, I, McCardle, J, Torrens, G, & Farrell, G. (2008). Mobile phone anti-theft designs: A review. *European Journal on Criminal Policy and Research*, 14(1), 39–60.
- Whitehead, S, & Farrell, G. (2008). 'Anticipating mobile phone 'smart wallet' crime: Policing and corporate social responsibility'. *Policing: A Journal of Policy and Practice, 2*(2), 210–217.
- Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime'. *Security Journal*, *14*(4), 63–82.

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at > springeropen.com