MOBILE TELEPHONE CRIME

- *Extent and cost of crime and fraud*
- *How it is perpetrated*
- *Potential measures to stop it.*

Mobile telephones are at the centre of a rapidly growing crime wave, costing £100-200M annually, with stolen mobiles even used as a criminal 'currency'. At the same time, the technological complexity of phone fraud makes detection and prosecution difficult. As a result, there are calls for new legislation to help curb the problem.

This POSTnote reviews mobile telephone crime and the policy issues which arise for Parliament.

MOBILE TELEPHONES IN THE UK

The UK mobile telephone industry involves many companies, large and small, grouped into four sectors: network operators, service providers, dealers and manufacturers. The network operators are licensed by the DTI under the Telecommunications Act 1984 and Wireless Telegraphy Act 1949, and regulated by OFTEL. There is no provision for licensing of service providers or dealers, although recently self-regulation hasstarted via the Federation of Communication Services (FCS). Many 'sub-dealers' however are not members of the FCS, so remain unregulated except for the provisions of normal commercial law.

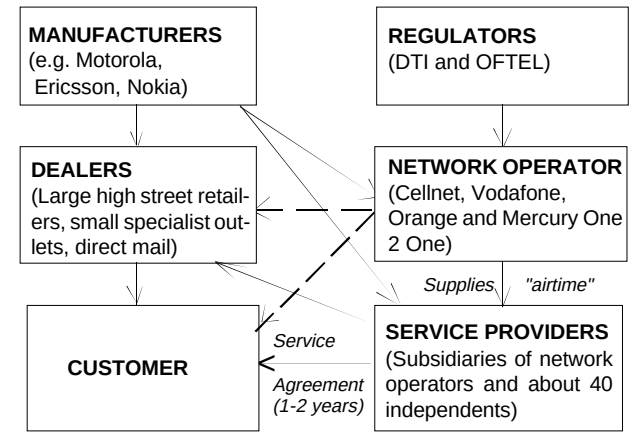
As far as the **network operators** are concerned, four companies run six networks under licence from the DTI. Cellnet and Vodafone each operate both analogue and digital networks, while Mercury One2One and Orange operate digital networks only; these networks and relevant technical details are described in **Box 1**.

The relationship between the four groups and the customer is illustrated in **Figure 1**. The initial network providers (Cellnet and Vodafone) were required until one year ago to sell airtime to subscribers through service providers (responsible for billing and the rental agreements etc.). The more recent network providers (Orange and Mercury One2One) have been allowed from the start to deal directly with their subscribers although they may also use service providers. An important feature of the mobile telephone market is the charging structure which stimulates rapid growth through incentives to service providers and dealers to sign up new subscribers. Service providers receive bonuses from the networks for signing up new customers and also charge a margin of 20-30% on the cost of calls. Consequently, large commissions filter down to dealers and customers - telephones which would retail at £250 are sold for £20 or less, provided the subscriber signs an airtime service agreement of 1-2 years.

POST note **64** **June 1995**

POSTnotes are intended to give Members an overview of issues arising from science and technology. Members can obtain further details from the PARLIAMENTARY OFFICE OF SCIENCE AND TECHNOLOGY (extension 2840).

Figure 1 STRUCTURE OF THE MOBILE PHONE INDUSTRY



Box 1 TYPES OF MOBILE PHONE IN THE UK

Analogue phones use the Total Access Communications System (TACS) standard, communicating via radio at a frequency of 900 MHz. As with a touch-tone terrestrial telephone, numbers are transmitted using special tones. Each TACS telephone is uniquely identified by its listed telephone number and an electronic serial number (**ESN**) which is set by the manufacturer. Both numbers are transmitted between a mobile phone and the nearest base station when a call is made or received, and every 30 seconds or so while the phone is switched on so that the network knows its location. Anyone with a suitable radio receiver ('scanner' costing around £1,000) can intercept any numbers that are transmitted. In the UK, there are two analogue operators: **Cellnet** and **Vodafone**; their networks cover over 98% of the population and together they have about 3.5 million subscribers.

Digital mobile phones convert all signals and numbers into a digital data stream for transmission. Advantages are:

- '**roaming agreements**' will eventually provide world-wide coverage (except Japan and the USA);
- digital signals are encrypted for high security;
- advanced features can be offered - e.g. paging and data links;
- sound quality is better.

Since 1994, **Cellnet** and **Vodafone** have been operating digital networks using the international Global System Mobile (GSM) standard (900 MHz). A GSM subscriber is identified on the network by a 'smart card' (SIM) which is what is registered with the networks and can, in principle, be inserted into any GSM telephone to make and receive calls. The **PCN** (Personal Communication Networks) operated by Mercury One2One and Orange are very similar to GSM, except that they transmit at 1800 MHz. Mercury One2One covers London, SE England and West Midlands (30% of the population), whereas Orange are expanding their network to cover 90% of the population by the end of 1995. About 650 000 digital mobile phones are currently in use.

MOBILE PHONE CRIME AND FRAUD

Against the backdrop of a market of dramatic growth (**Figure 2**), the main types of crime are summarised in **Table 1**, along with some of the consequences. **Theft** affects members of the public very directly, as well as the industry, whereas the main victims of **fraud** are the networks and the service providers.

Although statistics are not collected centrally, 12-15,000 analogue and up to 1,000 digital phones are believed to be **stolen each month**. Some theft is from warehouses, dealer premises or hi-jacking of delivery vehicles. But much is directly from the public, sometimes involving violence. Up to 40% of car break-ins in London are now believed to be for the purpose of stealing a mobile telephone, and the relatively new practice of 'jamming' (essentially a 'smash and grab' raid on an occupied car stuck in traffic) is increasing rapidly.

Two important factors underpin the rise in mobile phone theft. Firstly, it is easy to change the identity of most analogue phones by '**re-chipping**' (see **Box 2**), making it easy to re-cycle or export stolen phones and difficult to prove their origin. Secondly, compared with other electronic goods of similar face value (e.g. VCRs), for which a thief may receive about £50 from a "fence", a stolen mobile phone can attract up to a further £250 in commissions when it is reconnected to a network.

Mobile phone **fraud** is a more complex issue, but in almost all cases the goal is to make phone calls at someone else's expense - by '**cloning**' (see Box 2), or by obtaining a mobile phone from a dealer using a false identity (**subscription fraud**). Once obtained or configured to make 'free' calls, the phone can be sold outright or used to set up a **call-selling bureau**- anything from a single phone in the back room of a pub to a sophisticated dial-up service offering cheap international calls with total anonymity. The length of time such phones can be used before the fraud is detected varies from a few hours to weeks, by which time bills of several thousand pounds can be run up on one phone.

Subscription fraud affects the service providers directly and may in some cases account for over 5% of their turnover. With cloned phones, fraudulent calls are billed to the legitimate subscriber, although network operators generally detect that a fraud has taken place and accept liability before the bill is issued. Cloning is big business - the Departments of Health and Transport found 1% of their mobile phones cloned in 1994/5. If typical of national trends, and with average bills of £1000 (16 hours of international calls), the total value of fraudulent calls would be £70M per annum - consistent with the losses of 1% of turnover declared by the network operators. In addition to the direct crimes, mobile phones can have a role in other areas of crime. They render untraceable or unusable information gained by the police via call surveillance; they can also comprise a form of criminal 'currency', alongside drugs such as crack cocaine.

Figure 2 GROWTH OF THE UK MOBILE PHONE MARKET

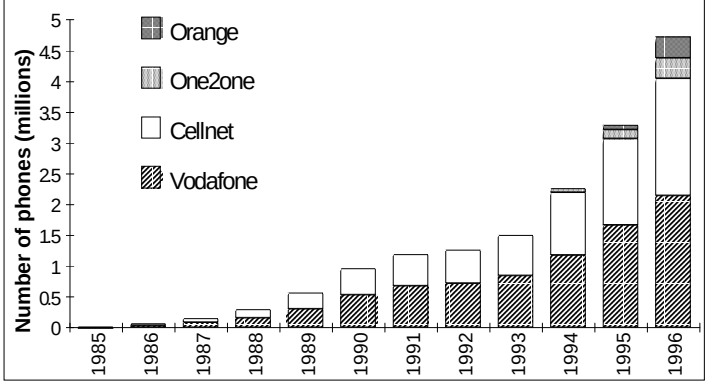


Table 1: SUMMARY OF MOBILE PHONE CRIME AND MISUSE

TYPE	CONSEQUENCES
Theft	Personal injury and/or damage to property. The owner must replace the phone, often costing around £250, or default on the rental agreement. The phone can be used to make 'free' calls until the theft is reported and the line is disconnected. The phone itself can be resold by the thief.
Cloning and Re-Chipping	A cloned analogue phone can be: used to make free calls; rented or sold to third parties to make 'free' (usually international) calls; used to call a premium rate (e.g. 0898) national or international number operated by or for a criminal, thus generating an untraceable revenue stream; used to make anonymous, un-traceable calls (e.g. to arrange drug deals).
Subscription fraud	Equivalent to theft; or the user can pay bills under the false identity for complete anonymity.

INDUSTRY SELF-REGULATION

Some industry practices and incentive structures create opportunities for criminals - e.g. the lack of physical identification marks on phones, the financial incentives for connecting a (stolen) phone, the ability to obtain a phone for a fraction of its real value. Thus the first response to concern over the rising scale of crime is to examine the potential for industry self-regulation.

The rapid growth in mobile phone crime initially took the industry by surprise and ever since it has been struggling to protect itself, with mixed results. As soon as one weak point is dealt with, others open up to the extent that some in the industry see themselves in a continuous 'guerrilla war' with the criminal community. For example, in response to the rise of subscription fraud, the service providers greatly limited the call facilities offered to new subscribers until the first bill was paid. This simple measure reduced small-scale individual fraud, but led instead to increasingly sophisticated fraud perpetrated by organised criminal groups, in order to obtain a stream of telephones for call-selling bureaus and export to other countries.

The FCS is leading an industry campaign to combat crime and has established a Crime Action Group (CAG) which brings together all sectors of the industry and the

Box 2 RE-CHIPPING AND CLONING

The electronic serial number (ESN) of an analogue, or the International Mobile Electronic Identity number (IMEI) of a digital, mobile phone is its unique identity and was originally intended to be inviolably incorporated into the phone. However, the security features which protect the number can be overcome and a new set of numbers installed. The change of identity is called '**re-chipping**' and can be achieved on analogue phones in a number of ways. Sometimes, the ESN can be altered directly from the keypad using supposedly secret combinations of keystrokes; in other cases, connection to a computer can allow the phone chip to be reprogrammed. The software to do this is available via advertisements in specialist magazines or even available free over the Internet.

Re-chipping is not illegal and was started to bypass the service providers when reconnecting a secondhand phone, replacing a faulty one or upgrading to a new phone. Once available, however, the equipment could be readily applied to give a stolen phone a new identity so it can be connected to a network, and to clone another mobile phone.

A **clone** is an analogue mobile phone which has been programmed to impersonate one owned by a legitimate subscriber by using its ESN and telephone number (these numbers are usually obtained by interception with a 'scanner' radio, theft of a dealer's or service provider's records or directly from the impersonated phone). New types are coming to the UK from the USA and Hong Kong: 'tumbling' phones automatically seek an identity from a pre-programmed list, and the most recent 'magic' phones act as their own scanners copying identities from nearby phones in use.

Police. The CAG sees **re-chipping as the fundamental issue** since this underpins both the re-cycling of stolen phones and cloning. The lack of regulation, especially at the dealer level also provides many opportunities for crime, particularly for trade in stolen phones, and in May 1995, the FCS announced they would be introducing a scheme for dealers, whereby dealers must check second-hand phones and allow FCS inspectors to check their documentation. One of the requirements of this code of practice is that dealers should consult a blacklist of stolen phones before accepting a 'secondhand' phone, and the FCS is pressing for all enquiries to the blacklist database to be logged, so that dealers can prove they have taken reasonable steps to ensure that a phone is not stolen. In return for these and other measures, accredited dealers may enjoy favoured status with the service providers. Such initiatives have to comply with EU / UK competition policy as overseen by OFT and OFTEL, and this may ultimately place limits on some forms of industry self-regulation.

The network operators and service providers are also developing techniques to combat fraud in all its forms. Their goal, of course, is prevention but in practice early detection to severely limit the potential fraudulent income may suffice. Cloned mobile phones can be detected by computer monitoring of call patterns where the software 'flags' unusual call patterns, allowing the legitimate user to be contacted and, if necessary, given a new phone. In addition, if the monitoring software detects two or more calls going on at the same time from the 'same' phone, clearly clones are involved (these are called 'call collisions'). However, the software challenges of these conceptually simple tasks are formidable with nearly 2 million phones on each analogue network. In order for call monitoring to be most useful, the service providers also need more direct access to network operators billing data, ideally in real time rather than with the current 12 hour delay. Another measure would be to provide free itemised bills (currently often charged for).

One solution to the problem of cloning would be to encourage a more rapid switch to digital phones, which are much more secure. They are however, more expensive to manufacture and in spite of their advanced features, most people believe that there will continue to be a strong demand for the cheaper analogue phones. Moreover, given the technological sophistication of some criminal elements, there is no guarantee that digital phones will remain immune from cloning, and there are already rumours that counterfeit smart cards for digital phones are being made in Japan. Vodafone are attempting to increase the security of analogue phones by using "*TACS Authentication*", which protects numbers in a similar way to GSM and is believed to make cloning more difficult. However, only 20% of the current pool of analogue phones support TACS authentication and these require adjustments which are not straightforward. This may thus be neither a quick nor comprehensive remedy to cloning.

Most industry measures to combat mobile phone crime require co-operation between all parties in the industry. The four network operators have agreed that "*security is a non-competitive issue*" and service providers increasingly are sharing personal credit information, subject to the scrutiny of the Data Protection Registrar. However, given the extremely competitive nature of the mobile phone market, many see significant limits to the extent and success of cooperative measures.

ISSUES

Is There a Role for a Tighter Regulatory Policy?

In response to pressure from the FCS and others, the Minister of Trade and Technology announced on 13 June 1995 the formation of a new Study Group to "*examine how best to work together ... to tackle the increasing problem of mobile phone crime*". The Group draws together the industry, DTI, Home Office and law enforcement agencies and will report in September 1995.

There is certainly scope within existing legislation for further public policy measures to reduce mobile phone crime. Even raising public awareness of the risks involved could have some impact since most people do not even take the simple precaution of locking their phone with a PIN[1] number. The regulators (OFTEL and

DTI) are concerned about mobile phone crime but have few levers on the problems; calls for increased regulation (e.g. by licensing service providers and dealers), are countered by those pointing out that mobile telephony's success arises from the large amount of lightly regulated competition, and consumers' interests may not be served by reducing that competition.

One regulatory **area of concern is over the issue of the unique identifiers** (ESN for analogue and IMEI for digital) and their subsequent control. At present, numbers are issued to manufacturers by BABT (British Board of Approval for Telecommunications) in much larger blocks than the number of phones actually made (to allow manufacturers to disguise their commercially sensitive production volumes), and this provides a large source of unused yet valid ESNs that re-chippers can guess easily. A reduction in ESN allocations may be too late in the case of analogue phones, given the millions already in circulation, but could be an important safeguard for the future of digital phones. In either case, there is a strong argument in favour of doing more to keep track of ESNs and IMEIs - not only those in use, but also those from phones which have been scrapped or stolen. The digital networks are at various stages of implementing whitelist / blacklist schemes, but these may be of little value unless similar precautions are adopted world-wide. **OFTEL could play an important role here as overseer of the system under which ESN and IMEI are issued**. However, the international dimensions of the problem suggest that other Government departments will need to be involved if ESN / IMEI control is to be effective.

An important role for public policy is to recognise the **growing social costs**, as well as economic costs, of mobile phone crime and to focus more energy on the apprehension and prosecution of those involved. A few Police Forces, most notably in Manchester, the West Midlands and London, have established specialist mobile phone task forces; in addition, all of the networks and some of the service providers have their own crime investigation services. These are all enjoying some success detecting mobile phone crime, **but find it very difficult to secure prosecutions** because often the legislation involved has been drafted before the technological complexity of this field was apparent.

For example, prosecution under the **Theft Act** is hampered by the difficulty of proving that a mobile phone is stolen once it has been re-chipped (the only unique identification number was its ESN which re-chipping has of course changed). Property marking schemes are helpful, but they are not widely used, and a better alternative could be a physical marking scheme analogous to that used for vehicle bodies and engines - e.g. by an identity number on the printed circuit board.

1. If a 'locked' mobile phone is stolen, the thief cannot use it to make calls without first keying in the secret PIN number set by the phone's user.

Likewise, use of a cloned phone is only an offence (under S42, **Telecommunications Act**) through it being "*fraudulent use of a telecommunications system*", but possession of equipment for cloning is not itself an offence. Similarly, possession of the equipment to eavesdrop is not an offence, so that contraventions of the **Interception of Communications Act 1985** and the **Wireless Telegraphy Act 1949** require the perpetrator to be caught 'red-handed'. Cloning may contravene the **Computer Misuse Act 1990**, in that the controls of a mobile phone are, in effect, a computer, making cloning equivalent to 'hacking'. However, so far the Crown Prosecution Service has declined to test this in court. Even the **Fraud and Counterfeiting Act 1981**, which was expected to be effective against counterfeiting of digital phone Smart cards, may not cover fraud perpetrated against the networks directly.

Proposals for New Legislation

The weaknesses in the coverage of existing legislation and the difficulties in obtaining prosecutions have led to calls for amendments to existing legislation. The primary proposal is to **make re-chipping unlawful except under a licence**, combined with making possession of unauthorised re-chipping equipment an offence. Such legislation was passed by the US Congress in 1994. Other proposals include:

- clarify existing legislation to make interception of network security data (e.g. ESNs) an offence;
- amend the Computer Misuse Act to explicitly include mobile phones;
- increase the penalties in the applicable Acts so that the offences are arrestable;
- make the possession of radio scanners capable of receiving certain frequencies an offence.

The Government remains to be persuaded of the effectiveness of further legislation on mobile phone crime, and this position is supported by some in the industry who are concerned not to impede the vibrant competition currently forcing it forward. Moreover, many point out that some of the crime is a direct result of industry practice and payment incentives, and there is still potential for further self-regulation to reduce the level of crime and fraud. As the extent of crime rises however, increasing numbers in the industry are concerned that voluntary measures cannot succeed while the law remains so ill-attuned to the nuances of such 'high-tech' crime. In view of the serious social consequences of this form of crime (Table 1), they argue that it is better to 'bite the bullet' now and modernise the relevant statutes than wait more years, so encouraging existing organised criminal activities to become even more institutionalised. These arguments will be aired in detail in the Government's recently-announced enquiry. More detailed briefing is also available from POST (extn 2840).