International Journal of Law and Information Technology, Vol. 6 No. 1

Techno-Cops: Information Technology and Law Enforcement

Amanda Hoey[1]

Abstract

Since the first wave of computerisation in the 1970's the implementation of information technology (IT) within policing has been chequered and often met with resistance. It was not until the early 1990's that IT in policing became a political issue of national importance within the UK. This culminated in September 1994 with the Home Office and the Association of Chief Police Officers issuing a National Strategy for Police Information Systems (NSPIS) for England and Wales. The development of an IT strategy must be viewed in the context of increasing expectations and pressure for reform within the police service as a whole and is set against a background of reports and studies aimed at enabling the police service to meet its aims more effectively. The business environment in which police forces operate is changing; increased demands for efficiency has led to IT being recognized as a valuable and innovative addition to policing. In recent years many technological developments have taken place initiated by local police forces themselves and by government both in the UK and the US. This article explores how technology can support the routine core functions of policing, the issues surrounding the use of the technology and finally draws some conclusions about the implications of the technology on the nature of policing.

Information technology has become pervasive throughout society and,

[1] LL.B, LL.M, PGCUT, Lecturer in Law, School of Public Policy, Economics and Law, University of Ulster at Jordanstown, Newtownabbey, Co. Antrim, Northern Ireland. BT37 0QB Tel:44 – (0)1232 368876 Fax: 44 – (0)1232 666847 Email: A.Hoey@ulst.ac.uk

indeed, has transformed much of the way we go about our work, whether it be in industry, education or the legal system. This article explores how information technology has impacted on a particular aspect of the legal system, namely that of policing and law enforcement. The article illustrates how police forces throughout the UK and US have put information technology (IT) to use and explores the extent of the role of IT within policing. Information technology is used in this context to describe the 'computerisation' of tasks which otherwise would have been conducted manually within the police service. Enhanced effectiveness and efficiency are generally accepted as the rationale for introducing technical change within any organisation, the police being no exception. Since the early 1970's the concept of 'computerized policing' has been evolving in line with technological advances and the changing nature of policing.

In the context of policing IT has been used to gather and manage all sorts of information (information management) and to facilitate the efficient deployment of manpower and enable quick responses (command and control).[2] The 1990's appears to have heralded a new era in computerized policing but it has been claimed that 'much of the recent innovation by the police seems to be motivated simply by the faith that the new technology must be helpful because it has been widely adopted by many other types or organisation'.[3] This undoubtedly is true but at the same time there has been a growing realisation within the police service itself that computerisation can lead to enhanced efficiency, competency and professionalism. This article explores the extent to which computerisation has pervaded policing and looks at current techniques which are in use and developments for the future.

1. Technology and the Nature of Policing

What do we mean by the term 'technology'? Within policing the term connotes many things, for example, probably one of the most well known and well tested pieces of police technology is the 'truncheon'. The introduction of radio and 'Panda' cars also represent technological developments. Police must respond to the needs of society and as the police develop in accordance with societal change they require new forms of technology to

[2] In the early 1970's the Home Office's Police Scientific Development Branch began developing command and control applications for police use. These applications consisted of Computer Aided dispatch (CAD systems which were designed to enable patrol cars to be dispatched more quickly to a scene once a radio call for assistance was received. The computer system provided information on the availability and location of patrols and once a patrol was dispatched details were recorded. Thus the system maintained a record of tasked resources for audit and the types and numbers of calls received.

[3] Ackroyd, Harper, Hughes, Shapiro & Soothill, *New Technology and Practical Police Work* (Open University Press: Buckingham 1992) at 71.

meet their objectives. The general assumption is that technology, in whatever form, represents a 'new tool' with which the police can operate more efficiently and effectively.

Three phases of technological development within policing in the UK have been identified: 'mechanized policing' (1960's to mid 1970's); 'fire brigade policing' (mid-1970's to early 1990's); and 'contemporary policing'.[4]

1.1 *Mechanized Policing*

The initial phase of mechanisation commenced with the introduction of panda cars and police radios. As crime rates increased, particularly in urban areas, police resources could no longer keep pace with the increased need. 'Bobbies on the beat' could not respond quickly to a call for assistance, say for example five miles away, whereas an officer in patrol car could be there in a matter of minutes. Thus a new method of patrolling was initiated which enabled flexibility and mobility and thus more effective policing. The traditional mode of policing continued but the way was being paved for a change in the style of policing.

1.2 *Fire Brigade Policing*

By the 1970's we saw the introduction of specialist police units and task forces. Whether it was the technology or societal change which precipitated these developments is open to debate but it is clear that both were mutually reinforcing. From the late 1970's to the mid 1980's police-public relations were generally at a low ebb, particularly in developing urban areas. There was increased sensitivity to the police which, combined with a more reactive style of policing facilitated by technological developments such as command and control systems, contributed to some of the worst clashes between the police and sections of the public ever witnessed.[5] This period of heavy handedness by the police force is generally referred to as 'fire brigade policing'. This period signalled a new style of police management which was very much interventionist.

Linked with this change in the nature of the police as an organisation there were technological developments designed to support the provision of a more effective and efficient service to the community. Since the early 1970's the police have been involved in the computerisation of tasks which otherwise would have been carried out manually. These tasks can usually be categorized in terms of administration or operational functions:

[4] Ackroyd et al at 71.

[5] In the UK for example, the industrial relations disputes 1978-79; the inner-city riots in 1981 and 1985.

(i) Administration:
Systems in this category support administrative functions in respect of statistics, record-keeping, office automation and the like. These systems tended to replicate traditional manual record-keeping systems and support services. The majority of them emanate from the first wave of police computerisation in the 70's and 80's.

(ii) Operational:
Operational functions comprise management of the organisation and a facilitation of the performance of the duties associated with being a member of a police force. This category includes systems such as Command & Control, duty rosters, criminal intelligence, major incident inquiries, to name but a few.

1.3 *Contemporary Policing*

'Contemporary policing' is difficult to categorize as many varying styles of policing are evolving. However one common thread appears to be that it is increasingly being recognized that IT is the way forward for policing in general:

> The police have traditionally been encouraged to invest in people rather than technology. Because of this we have reached a point of imbalance where we realize we need to invest more in IT to empower the ordinary constable doing his or her job.[6]

The history of computerisation within policing throughout the world has been chequered and often met with resistance. Why have the police in general failed to accommodate technological change? The two main reasons for this are police culture and lack of funding. Most police officers have a distaste for office life, preferring to be out 'on the beat'. Computerisation is seen as a threat to traditional 'beat style' community policing and the autonomy of patrolling officers. For example, in Boston (USA) the introduction of a computer aided dispatch (CAD) system in the early 1970's was abandoned as an 'unjustified interference in patrol officers' ability to determine when and how work should be performed'.[7] Patrol officers resented the fact that the system explicitly provided information relating to their activities to their superiors in that speed of response and numbers of responses made by each patrol unit were monitored. Interestingly the introduction of patrol cars was also viewed with similar hostility and scepticism yet patrol cars are nowadays an indispensable policing commodity. The

[6] Assistant Commissioner Peter Winship, Chairman of ACPO's Technical and Research Committee, Computing, 14 April 1994.

[7] Ackroyd et al at 84.

introduction of such technology was unavoidable in the context of a changing society with increased car ownership, urbanisation and increasing crime rates.

At the same time financial constraints are evident. For example, in comparison with industry in the period 1990/91 the overall spend on IT within the Computer Services of the Royal Ulster Constabulary (RUC) was £4m. This amount represents approximately 0.8% of the total organisational expenditure whereas the industrial average was between 2-4%.[8]

Despite the fact that these barriers exist, however, many developments have taken place initiated by local police forces themselves and by government. Various examples of how sophisticated technology can be connected to the functions of policing are provided in this article as it explores how technology can support the routine core functions of policing.

The main aim of a police force in general is to prevent and combat crime and to provide an efficient and effective service to the community. How then do the police go about their routine tasks with the aid of technology?

2. Cracking Crime with Technology

Policing tasks include service delivery, strategy development and the provision of support services. Within the context of delivering a service to the community technology can be used in a variety of ways. The police need information in order to do their job. Police detect very little crime themselves but rely heavily on information from the public about the commission of crimes. Also in order to plan operations, surveillance or identify likely suspects in a criminal investigation they will need information such as geographic details, physical descriptors and the like. Technology can be used in order to enhance the operational effectiveness of the police by allowing vast amounts of information to be stored in readily accessible form and enabling the police to deploy resources efficiently and finally by aiding the police in large scale preservation of law and order. The core function of policing is to prevent and combat crime and this section explores some of the uses of technology in this area. The key activities in which the police will be involved comprise investigation, patrolling, gathering intelligence, crime analysis and surveillance.

In developing strategies, whether it be for a small scale operation or the management of the police force nationally, technology again comes into play. Computer applications relating to crime analysis, command and control, mapping, surveillance and administration may be useful in this con-

[8] Figures taken from 'An Information Systems Strategy Scoping Study for PANI and the RUC' November 1991 (The Griew Report).

text. It is clear that some of the techniques described in this article may be of use in a variety of contexts and there will be an overlap between the functionality of the technology in service delivery and strategy development. The third area of activity is the provision of support services. In this field technology is used for efficient management and administration purposes. This article concentrates on how information technology is used on an operational basis in order to crack crime.

3. Investigating Crime and Responding to Incidents

In providing a service to the public the police are required to investigate crime and respond to incidents. The basic tenet of policing is to prevent and combat crime. Information technology has impacted greatly on this aspect of law enforcement with computer applications developed to support the functions of identification, gathering information/intelligence, crime analysis, command and control, mapping and surveillance, all of which are essential to aiding the prevention and combat of crime.

3.1 *Identification*

Identification is a key process in any criminal investigation. In order to crack crime the police need to hold information on individuals, property, vehicles and the like to which in the event of an incident cross referencing can be made. Computerisation of these records and incident logging is for the purpose of identification and apprehension of criminals, identification of stolen property and to enable information to flow freely between police forces. Time consuming manual record checks are eliminated and thus the police can operate more quickly and efficiently.

One such example of a system designed to facilitate these objectives is the UK HOLMES system (the Home Office Large Major Enquiry System).[9] This is a standard Home Office system contained in nominated incident rooms

[9] This system is the direct product of public outcry over police handling of the 'Yorkshire Ripper' case. It was clear from a series of murders perpetrated in the North of England in the 1970's that they were the work of one person. It was only after fourteen women had died that Peter Sutcliffe, the 'Yorkshire Ripper' was convicted. During police investigations of the murders information was recorded manually by several of the forces involved in the hunt for the killer. This information amounted to hundreds of hand-written cards containing details of vehicles, sitings etc. which made it difficult to retrieve and any search was likely to be extremely time consuming. After the arrest and conviction of Peter Sutcliffe it was discovered that he had in fact been arrested on several occasions by officers from different forces but released each time. The amount of the paperwork involved in the enquiry was identified as one inhibitory factor, amongst others, in the efficient handling of the investigation. As a result of an inquiry into the case HOLMES was introduced.

throughout the police forces in the UK. Each incident room has its visual display units and printers connected to the mainframe at Hutton by telephone lines. The aim of this system was to enable standardisation of incident recording and administration. It contains and processes all information regarding major incidents. It consists of sophisticated software which provides a log and database for incidents which can be accessed from any HOLMES incident room in police stations throughout the UK. HOLMES is a very important part of any major crime investigation, for example, it was used for logging information concerning Fred and Rosemary West's crimes.

In order to eliminate endless hours of searching by police officers each regional HOLMES database records details of major local crimes which can then be accessed via the dumb terminals in other police stations. Despite saving time when investigating major crimes the system does not actually allow different police forces to link information. In line with the National Strategy for Police Information Systems (NSPIS) launched at the end of 1994 the Home Office decided to review currently available systems. The basis of a National Police IS/IT Strategy rests on the premise that all police forces carry out same processes therefore it should be possible to define a common set of information systems to support those processes rather than having forces individually defining their own. Under the auspices of the NSPIS a reincarnation of the major investigation system will be rolled out in early 1998. This system, HOLMES 2, will do everything which the original system did but will be easier to use. For example, originally four suppliers provided the systems for the database which caused problems if one force was trying to access information from another force database provided by a different supplier. HOLMES 2 will allow forces to automatically link incident information since only one supplier has been contracted to develop the system. HOLMES 2 will also be run on PC's, unlike the original dumb terminals, and thus access and ease of use is greatly facilitated. The use of standardized software which can integrate with other systems already in use should undoubtedly free up officer time on major investigations and enhance the overall efficiency of any major investigation.

3.1.1 *Biometrics Verification*

Apart from being able to identify individuals via physical descriptors such as weight, hair and eye colour one particular technique which merits attention is that of biometrics verification. This is the terminology used to describe the technique of identifying individuals by unique physical characteristics. This technique was initially pioneered in criminal investigations since the late 19th century with manual fingerprinting of suspects which could be matched to fingerprints found at the scene of a crime. As a result of technological innovations this technique has developed into a highly sophisticated state of the art identification mechanism. Computerisation

now enables electronic scanning and digitalisation of fingerprints. Automatic Fingerprint Recognition (AFR) is a form of biometrics verification. The introduction of the National Automatic Fingerprint Identification System (NAFIS) in the UK will allow automated matching of fingerprint images in the national collection of fingerprint records. This system is due to take over in all forces in England and Wales in 2001 and in the meantime the AFR consortium led by the Hampshire Constabulary has contracted with an American company to provide an AFR system for 33 of the police forces.[10] As well as permitting identification of suspects fingerprinting can be used to help combat fraud, for example in California and New York all welfare beneficiaries and their families are fingerprinted. California also requires drivers licences to incorporate thumb prints.

DNA Databases are a further extension of biometrics verification: they enable individuals to be identified via genetic makeup of samples of body hair, tissue, saliva etc. Both within the UK and USA genetic profiling has become a reality. In the USA the FBI has spent millions of dollars creating a computer network to link all US states databases and form one central registry. Universal tracking is thus becoming a reality. Usually in the context of a criminal investigation the targeted individual knows that he or she is being checked and is usually required to co-operate. Developments such as facial recognition and facial thermography would permit more covert identification. This technique is discussed further in the context of surveillance technology (below).

3.2 *Gathering Information/Intelligence*

Gathering information has been identified as a key process in policing and once this information is gained it need to be stored. From the early 1970's technology has been implemented to enable the storage and processing of information. Police need information about people (physical descriptors), places (geographic descriptors), vehicles, movements of individuals etc. in order to carry out their job. Computerized storage of such information has inevitably impacted on the style and quality of service to the public. Police no longer need to laboriously wade through disparate files in various locations – computerisation has facilitated ease of access to such information and hopefully as a result a more efficient police force. On a national level police forces within the UK have access to the Police National Com-

[10] The development of an AFR system has been plagued with problems. The AFR consortium terminated its contract with IBM in March 1995 due to the fact that the system did not work properly. A temporary US-based service was in use until finally in September of last year the consortium contracted with North american Morpho Systems (Nams). This contract is due to run until 2001 when the NAFIS system will take over. Currently the AFR consortium and IBM are suing each other.

puter (PNC) which is probably one of the most well-known and most commonly used police IT applications nation-wide.[11]

3.2.1 *The Police National Computer*

In 1995 the PNC celebrated 21 years in operation. The PNC is operated and controlled by the Hendon Data Centre (HDC), London and is directly connected to force terminals. The HDC is constantly striving to enhance IT facilities available nation-wide to the police force. The centre's purpose is 'to deliver approved police national information systems to performance standards specified in the service level agreement with police service users'.[12] (Police Department Command Plan 1995/6). The PNC comprises a highly sophisticated system which contains eight applications; vehicles, names (Phoenix), fingerprints, property, broadcast, transaction and message logging, directory, and crime pattern analysis.

The use of the PNC facilitates information matching, surveillance and communication between forces on a national level. It is claimed that the PNC enables the police to implement strategies and tactics which would otherwise have been unavailable to them under the old manual systems. For example the 'vehicles application' contains information on vehicles, current owners and searchable register of vehicles stolen, lost or in which police have an interest. The application was introduced in 1974 and currently 'Vehicle Owners' contains approximately 42m records. Information is provided by the Driver Vehicle Licensing Agency (DVLA); new registrations and changes to vehicle owners are recorded by DVLA five days a week and this information is transferred to Hendon. Some of the information held on the system may be out of date because the update is not received by Hendon until at least one day after they have been processed at DVLA. Regional and local police forces also provide information on stolen or suspect vehicles.

On an operational level the vehicles application may assist the ordinary officer in the carrying out of his duties. For example, if a traffic branch officer sees a car being driven in a suspicious or erratic manner he can easily radio his divisional headquarters and request a PNC check on the car. This check will be conducted by an officer at the PNC terminal in headquarters which is linked to the PNC. The check will be initiated by entering the registration number of the car. In a matter of seconds details will be provided on the screen on the make, model, colour, name and address of owner and

[11] Usage of the PNC for 1995 totalled 50,093,063 transactions which was a new record (first time over 50 million) and indicated a rise of 5.6% over the 1994 total. HDC Annual Performance Report 1995, Home Office Police Department Science and Technology Group.

[12] Police Department Command Plan, 1995/96.

whether the vehicle is 'of interest to the police'.[13] The operator then relays this information to the officer on the ground who can then take the appropriate action which is usually to stop the car and request the drivers details. If the driver is the owner of the car then the details available to the officer will be confirmed but on the other hand the driver of the car may have stolen the vehicle and as such is not likely to know the owner's name and address. Thus the technology in this instance enables the police to apprehend criminals who otherwise would have 'got away with it'. The use of the technology also represents a change in police procedure since in order to catch a 'car thief' an extremely large number of checks will have to be conducted with the result that many of the checks actually conducted will be speculative. Particularly in Northern Ireland with the terrorist threat police traffic checks are all too common place and when conducted on an organized and large scale can be disruptive to motorists. However whether such checks are on an ad hoc basis or part of a planned operation it is clear that they constitute an unavoidable side-effect in the fight against crime.

Another significant feature of the PNC is the 'names application'. As it suggests this application relates to individuals and contains three elements:

(i) Criminal record information e.g. name, date of birth, aliases, details of convictions etc, including Criminal Record Office Number(CRO).
(ii) Wanted /missing persons information which also includes persons wanted for non-payment of fines, failing to appear in court, absent without leave (AWOL) etc.
(iii) Details of those disqualified from driving.

Access to 'Names' via the Criminal Record Office number will give full details of criminal records held by the National Identification Bureau (NIB). The application helps police officers to identify missing/wanted persons or those disqualified from driving. This information is available on-line to police forces.

1995 saw the advent of 'Phoenix', the new police database which holds detailed information on known associates, habits, full arrest detail, places frequented, court results etc. The wanted/missing persons and disqualified from driving information similar to that contained on the old names application is retained but now the application also hosts nominal records, which consist of a personal identification number and about 200 items including subject name, nicknames, aliases, date of birth, full description, last known address, information on impending prosecutions, court appearance dates, convictions etc. Reference numbers such as arrest summons reference number and CRO numbers are accessible. Phoenix pro-

[13] Perhaps the vehicle belongs to someone known to the police to be involved in crime or belongs to a particular individual who is under surveillance or the vehicle itself has been used for criminal purposes before.

vides an overview of information collated, together with a warning, intelligence and interest markers. Phoenix now allows police officers direct access to a wealth of personal information previously only available by postal enquiry to NIB. The new Phoenix facilities speed up enquiries and the identification of suspects. They represent major crime -fighting advantages to the operational police officer. It is also intended that this database will provide the basis for future advances such as keyword or speculative searching. Future developments include an extended names search facility which will permit a search of the national collection of records for crime investigation purposes and identification of offenders. The scope of the application will also enlarge to include details on minor offences, cautions, firearms owners and will also include photographic images.

3.2.2 *Concerns about the use of the PNC*

Despite the fact that undoubtedly these facilities are beneficial in terms of policing they have given rise to concern about individuals' privacy. Most of the criticisms surrounding the PNC relate to the nature of the information held on it and the use to which that information is put. The PNC is exempt from the controls over sensitive data that apply to other systems and as a result it may with impunity collect information about racial origin, political views, health, sex life, and criminal convictions.[14] Personal information about witnesses and victims are stored as well. In the absence of rigorous supervision this represents a potentially sinister feature of police control. As one commentator points out 'almost 120,000 calls are made to the PNC every day, but few are monitored to ensure that the request is bona fide, despite the inevitable Home Office Guidelines'.[15] Millions of people are checked against the PNC annually, most of them by officers on the street. Approximately nineteen million vehicles are checked against the PNC every year; almost all these checks are on vehicles which are neither stolen or wanted.[16] Again most of these checks are by officers on the street and access to the information is via the vehicle registration number or ID number and its make. The use of the PNC by the police came under scrutiny in the recent case of *R v Brown.*[17] In the context of data protection only information which is within the register entry is permitted to be stored and it is an offence to act outside the register entry. In the *Brown* case it was alleged that a police officer had 'used' information contained on the PNC relating to the ownership of two cars contrary to s. 5(2)(b) of the Data Protection Act 1984 (DPA) i.e. for a purpose other than that contained in the register

[14] Under the Data Protection Act 1984 'national security' provides a catch-all exemption from the provisions of the Act. In relation to the PNC, individuals, or 'data subjects' as they are referred to under the legislative provisions, have no right of access to information held therein.

[15] Robertson, *Freedom, The Individual and the Law* (Penguin: London 1993) at 121.

[16] Robertson at 121.

[17] [1996] 1 All ER 545.

entry. The police officer was involved with a debt collection agency and he accessed the relevant PNC details of two cars belonging to individuals who owed money to the agency. The information had only been retrieved on to a screen and there was no evidence that the information had subsequently been used. At first instance the officer was found guilty but the Court of Appeal upheld his appeal and the case then went to the House of Lords. The crucial issue was whether in the act of retrieving the information the officer had 'used' the information. Regrettably it was held that the action could not be interpreted as actual 'use' within the ordinary dictionary meaning of the word. Lord Griffiths, dissenting, claimed that this narrow construction of the word 'use' defeated the purpose of the DPA which he asserted was to protect individual privacy. As Ian Walden rightly points out, 'the decision has been seen as a serious limitation on the protection afforded by the Act and the ability to bring criminal prosecutions'.[18]

Another worrying aspect is that in 1990 Parliament's Home Affairs Committee discovered that Government Departments and agencies had checked police records on over half a million job applicants and the Committee expressed alarm at the high level of inaccuracies contained therein. A high profile difficulty was the inclusion of an individuals HIV/AIDS status as part of the contagious disease warning on the PNC. These references have now been removed since the Data Protection Registrar felt that inclusion of this information would have been in breach of one of the Data Protection Principles with which by law users of data held on computer are supposed to comply.[19]

3.3 *Crime Analysis*

Linked with the identification of suspects Crime Analysis applications may also be useful. For example the Crime Pattern Analysis component of the PNC contains files of crime reports regarding murder, sexual offences, burglary, robbery. Its purpose is to facilitate the comparison of similar crimes on a national basis and to enable identification of offenders or discover other offences committed by persons recently arrested. Information on the application is provided by five regional National Criminal Intelligence Service (NCIS) Officers in England and Wales, NCIS Headquarters and the Scottish Crime Squad in Glasgow. Searching can be carried out on the basis of free text searches or keywords. The application was introduced in 1983 and details of all unsolved murders since 1974 are on file. It is used by NCIS Headquarters and the five regional offices of NCIS and Scottish Crime Squad via dedicated PNC terminals in their premises.

---

[18] Walden, in *Computer Law* (ed C. Reed) (Blackstone Press Ltd: London 1996) at 350.

[19] In the 11th Report of the Data Protection Registrar June 1995 (HMSO: London 1995) at 30 it was pointed out that 'the inclusion of the information, had it been maintained, would have been in contravention of Principle 4 which requires that personal data held for any purpose or purposes should be adequate, relevant and not excessive in relation to that purpose or purposes.

Within the US similar developments have also been taking place. Some of the most significant projects have been conducted under the auspices of the Institute of Police Technology and Management. The Institute was set up in January 1980 'for the purpose of providing management, traffic and speciality training to municipal, county, state and federal law enforcement officers'. The Institute is part of the University of North Florida and one of its main roles is to apply computer technology to law enforcement and highway safety in the US. In the field of crime analysis one of the most widely used systems is 'MECCA'.

This is a powerful programme designed using artificial intelligence concepts which permits most primary suspect-offenders matches. The system contains analysis on crimes like burglaries, robberies, vehicle thefts and sex offences. The factual/geographic information relates to premises, locations and suspects' actions. This information is modifiable which means it can be adapted to suit individual users needs. Another feature of the system is built in pick lists, for example hair and eye colour may represent one set of values within certain fields. The user selects a particular crime to analyse, for example vehicle thefts, and then enters the data. Once information is entered into the system, for example details of the location of a crime, the type of crime committed and physical characteristics of the suspect, a report is produced. This report comes in two parts:

(i) a detailed breakdown of the particular crime comprising quantity and percentages relating to time of day, day of week, premises and geographic location etc.
(ii) matching the suspect to known offenders.

Thus the system enables the police officers to target particular offenders and conduct their enquiries accordingly. At the time of writing the cost of this system was $2400 irrespective of the number of computers or networks to be used. This undoubtedly represents value for money and puts such a system within the reach of police departments with a limited budget.

3.4 *Command and Control*

A routine policing task is to 'respond to incidents'. This can range from sorting out domestic disputes to controlling a confrontation at a large scale demonstration. All emergency calls for help can be made via the operator by dialling 999 – where do these 999 calls go and how can computer technology help the police with this routine task?

Until the early 1980's if a 999 call was made to a police force the procedure for following it up would have been conducted manually. For example, until 1984 any 999 call made to the police in London (Metropolitan Police) would have been handled in the following manner. An officer would take the call and write down the details on a pre-printed card which would then be transferred to a 'despatcher' (the officer responsible for deploying police manpower). The 'despatcher' would then radio the patrol

cars in the specific area and offer the 'job' to whom ever could take it. The card would then be passed to a 'logist' who would ensure that the requisite action had been taken i.e. an appropriate response made to the call and would then store the card in the manual filing system.

In October 1984, however, all this was about to change. The Metropolitan Police had installed a new Command and Control (C&C) computer. This eliminated the need for the manual card filing system and instead all details of calls received would be henceforth keyed into the computer which would then provide the operator with details of patrol cars/officers in the specified location and enable the deployment of manpower almost immediately. The details on such C&C computers are constantly updated by the routine calls made to headquarters by officers on patrol. Thus we can see that the function of a C&C computer is essentially twofold; to monitor police resources and to deploy police resources.

In fulfilling these functions the impact of such systems on police procedure has been significant. C&C facilitates tighter control by senior officers over day-to-day police work. This enhanced organisational power is attributed to the nature of the C&C systems on which vast amounts of information is held concerning activity in the community and movements of the officers whose job is to police that community. This monitoring ability allows senior officers to know precisely what is going on and where. It also facilitates analysis to determine where and when crime most likely to occur. Computerisation in the form of C&C also facilitates a quick response to calls for assistance. Overall the main advantage of C&C is the efficient deployment of resources and manpower.

Many of the systems are based on military style applications which has led to a move towards a more military style policing. This is reinforced by enhanced police communications. The concept of 'message switching' is simple – an individual officer at a computer terminal in one police station can send a message to another officer at another terminal at a different station within the same force. These messages are continually tracked. On a broader scale 'message switching' can be used to transfer messages within different forces since it is not dependent on the same machines or software etc. 'Message switching' can even take place via a 'connecting machine' such the PNC which contains a 'broadcast' facility which essentially allows for transmission of messages to connected terminals.[20] In this context it has been claimed that:

> The C+C computer is doing more than providing a rapid response to 999 calls, more than logging information, more even than forming a rapid

[20] This facility can be used both for small scale local control or on a larger scale for the control of a national situation. Indeed it was the 'broadcast' facility which was used during the 1984-85 miners' strike to instruct local police forces from the National Reporting Centre and to keep them informed about pickets' movements.

and more accurate communications network. It is making the police command structure more centralized and its style of operation more militaristic. These systems are starting to provide the electronic sinews of a Big Brother society.[21]

3.5 *Computerized Mapping*

Computerized mapping is not a new phenomenon and the use of the computer in this manner is evidenced from the early 1960's. However it is clear from research findings that it is only in recent years that usage of this technique has become widespread largely due to the advent of relatively cheap software. In a recent article[22] published in July 1995 as part of the US National Institute of Justice (NIJ) 'Research in Action' Series the author looks at organisations which use mapping technology for crime control and prevention purposes. The effectiveness of this technique is assessed and obstacles to the use of mapping are identified. In particular, police departments merit detailed attention as common users of mapping software and it is interesting to explore how such software is used and the effectiveness of its use within policing.

In the field of crime control and prevention the information contained on a mapping system will invariably include the location of a crime, the location of individual(s) who report the crime, the location of any recovered property, any last known addresses of the perpetrator and of his known associates, the location of previously committed crimes and particular conditions in an area.

All this geographic information helps build up a picture of where crime is likely to be committed and the type of crime committed. This information can then be used in trying to catch a suspect or when designing crime prevention programs for particular areas. Other information which may be useful in building up a fuller picture comes under the heading of 'social data' such as unemployment rates, vacant property, drug activity etc. The main feature of a mapping system is that it allows a multidimensional view of criminal activity in a particular location. Both the geographic data and the social data represent variables and layer upon layer of information is built up until you have different sets of data combining to present the overall picture based on different sets of variables.

It has been claimed that:

> The potential for institutionalized use of mapping software is far greater in police departments than in other organizations involved in crime control and prevention activities because computerized

[21] British Society for Social Responsibility in Science (BSSRS) Technology of Political Control Group, *Technocop: New Police Technologies* (Free Association Books: London 1985) at 63.

[22] Rich, 'The Use of Computerized Mapping in Crime Control and Prevention Programs' (1995) *NIJ Research in Action.*

"geocoded" data are the byproduct of routine, day- to-day police department work. Computer-aided dispatch (CAD) and records management systems that store and maintain call-for-service, incident, arrest and other potentially mappable data are now common in most medium and large police departments.[23]

Four main user categories have been identified within the police in general; these comprise planners, researchers, patrol officers and dispatchers.

3.5.1 *Planners*

The most common use of mapping software is in the field of crime analysis. Mapping is the term used to describe the pinpointing of various forms of crime on a 'map' originally using coloured pins to illustrate the periods in which crime occurred and in which locations. We are all familiar with the use of 'pin-maps' to illustrate the level of criminal activity in a given location. Computerized mapping has been described as 'a natural extension of the paper pin-map that offers far greater flexibility and analytical capabilities'.

Mapping can be used for operational planning in that it can assist in picking out areas for operations, for example the data stored on a system can give a profile of particular crimes perpetrated in particular areas and as such the planner can identify areas of particular need.

Mapping is also of use to the officer who is on patrol since the system can provide an overall picture of criminal activity in the patrol area.

The extent of the use of mapping varies within police departments, for example, San Diego and Los Angeles which would be categorized as two of the larger police departments in the US, use mapping on a routine basis closely integrated with CAD software to which the mapping information is transferred electronically. Some of the smaller departments use mapping independent from CAD, for example, Rich cites the example of Vacaville, California in which the crime analyst prints out daily the list of calls for service received in the preceding 24 hour period. Certain selected calls from the CAD system are then entered by the analyst into a database and then a mapping package is used to manipulate the data into crime alert maps. This exercise is time consuming, taking approximately 3 hours per day, but it is a valuable and relatively inexpensive (the mapping system only costs $3,300) mechanism to assist in operational planning.

3.5.2 *Researchers*

In this area a particular system has been developed under the auspices of the Bureau of Justice Statistics and researchers at the Illinois Criminal Justice Information Authority. The package is called Spatial and Temporal

[23] Rich at 3.

Analysis of Crime (STAC) and is used to identify 'clusters of criminal activity'. It is not a mapping system as such but is an analysis system which produces results which are then fed into the mapping system to show the areas of activity. In 1995 115 organisations were using STAC, 69 of which were police departments.

3.5.3 *Patrol Officers*

One particular development by the Chicago Police Department (CPD) which deserves to be mentioned is 'Information Collection for Automated Mapping' (ICAM). Using ICAM patrol officers can produce their own maps without needing to have a degree in computer science. All the officer has to do is use the mouse to click on an incident type, name of an area, type of location etc. The officer can then access a list of the top ten crime problems on specific beats. The information contained in ICAM comprises the previous two months data on crime which is transferred automatically from CPD's main record system to ICAM. What the patrol officers have is essentially a user-friendly, speedy and up-to-date means of accessing information on the incident of crime within particular locations.[24] This information can then be used to determine the areas of most criminal activity or where more serious criminal activity is located and thus will help determine where the necessary manpower is deployed. ICAM is an integral part of CPD's community policing programme, Chicago Alternative Police Strategy. In the context of community policing innovative approaches are required to enhance the provision and analysis of relevant information which can then be of use to police officers on patrol within the community – ICAM is just one example how technology can be used to make routine community policing more effective.

3.5.4 *Dispatchers*

Mapping can be used to increase the effectiveness of dispatching and thus create a more efficient police force. Dispatchers are aided in their role by immediate access to the location of a call for service which is displayed on the mapping system and supplemented by information the locations of patrol cars and other response units. Using this technology enables the dispatchers to quickly target the nearest patrol cars, deploy them to the location of the incident and thus speed up response time.

Mapping software can also be used for other purposes not directly related to crime control or prevention, such as tracking missing children and monitoring probationers. It is clear that mapping software can be

[24] ICAM is installed in all 25 of Chicago Police Department's stations and is available via laptop computers in over 3,000 patrol cars.

extremely beneficial in improving performance, a continuous objective of police departments in general.

3.6 *Surveillance Technology*

Other forms of technology such as video surveillance are also becoming increasingly significant as both a means of crime prevention and detection. In the performance of routine policing tasks CCTV can provide greater reliability than its human counterparts as the machines can record activity on a twenty four hour basis and do not need to be continually manned. Surveillance cameras are all over the place in public areas, car parks, housing estates, public amenities etc. Whether we know it or not surveillance has become part of our daily life. The use of CCTV has been pioneered in the UK by the Home Office Science and Technology Branch. CCTV is sophisticated technology used to monitor activity in a particular location and may incorporate various features such as night vision, computer assisted operation, zoom facilities etc. The technology was an initiative born out of football hooliganism in the UK and in 1985 a grant was given to football grounds and police forces by the Football Trust to commence a programme of gradual introduction of surveillance systems in and around football stadiums. The effect of this initiative has been dramatic. Currently there are approximately 300,000 cameras in over 100 UK towns and cities operated by the police, local authorities and private industries. In monetary terms in the range of £150m – £300m ($225m – $450m) per year is spent on surveillance. The UK has lead the way for the implementation of this technology and has to date been followed by North America, Australia and some European countries.

In the context of policing the justifications for using CCTV are :

1. to reduce or prevent crime,
2. to deter criminal activity,
3. to help secure convictions, and
4. to add information to police files regarding suspicious activity.

There is a debate over how effective the technology is in preventing crime. The statistics show that the effect on crime is evident and the technology appears to be most useful in the areas of car theft, assaults and ordinary theft. However these statistics can not be looked at in isolation since certain factors may cloud their reliability. In a recent Home Office Report[25] it was revealed that CCTV may not be as effective as the statistics tend to suggest. Serious shortcomings were identified in that levels of crime in particular areas were seen to drop irrespective of whether CCTV surveillance was operable or not. Also it is arguable that certain forms of crime have been displaced to other areas out of sight of the cameras since CCTV is

[25] Paper No. 68 in the Crime Detection and Prevention Series.

usually located in high rent commercial areas. This may be true but despite the unreliability of statistics CCTV does represent a new concept in technology which can help the police carry out their job more effectively. Indeed it has been shown that once crimes are detected on CCTV the conviction rate rapidly increases. Anyone caught on camera or who thinks they have been caught on camera will usually enter a guilty plea.[26]

CCTV has become so commonplace that it is now an integral part of law enforcement strategy. It provides for a different form of policing in that the technology can be used to police public morals and public order.[27] Indeed it has been claimed that 'the technology has had more of an impact on the evolution of law enforcement policy than just about any technology initiative in the past two decades'.[28] The use of the technology, however, has been a contentious issue. There are the widely acclaimed success stories such as the identification of toddler Jamie Bulger's murderers and the first Oklahoma bomber, all caught on CCTV. The technology did not prevent the crime from taking place but did contribute significantly to the apprehension of the suspects.

The main criticisms of the technology reverberate around cries of 'invasion of privacy'. Privacy International[29], a human rights organisation concerned with privacy, surveillance and data protection, has expressed concern that the implementation and operation of CCTV is largely unregulated. One of the main concerns of Privacy International is the development of 'Computerized Face Recognition' (CFR) systems. These computer systems can compare faces captured on CCTV with facial images kept on a database, for example, within police departments. Facial recognition involves measuring the curves on the face from several angles and then digitilizing the measurements and then doing a comparison with images already held in a database. Claims by Neurometric, a Florida manufacturer, state that images in a database of 50 million faces can be compared in seconds. Facial thermography relies on the heat patterns emitted by each face. In this area it has been claimed that developments are surpassing the traditional methods of identification in respect of their accuracy. Such systems are currently also surprisingly cheap. Mikos Corporation's Facial Access Control by Elemental Shapes (FACES) costs only $1,000 and as such it would be feasible to see such mechanisms being used in automatic teller machines, computer networks, point-of-sale terminals etc. The only drawback of the systems seems to be that their accuracy levels are affected by

[26] In Newcastle it has been reported that since the introduction of a 16 camera system in 1992 there has been 100% guilty pleas.

[27] It is usually 'low level' crime such as vandalism, fighting, drunkeness and sexual harrassment which comes under scrutiny and not burglary, assault and theft which were the originally targeted crimes.

[28] Privacy International Statement on Closed Circuit Television (CCTV) Surveillance Devices, October 14, 1995.

[29] Set up in 1990 and is based in Washington DC with offices in London and Sydney.

alcohol consumption. Calls have been made for relevant safeguards to be imposed regarding the use of the systems and even the possibility of a watchdog body set up by the government to monitor the systems and to recommend appropriate legislation to govern the use of such systems. A Code of Practice has been issued by the UK Home Office but the area still remains unregulated. The police response, however, to the issue of individuals' privacy would be that in providing CCTV public places are made safer and thus public freedom is enhanced. Also recent research has shown that these privacy fears are generally overridden by public perception that these systems are 'good' and will benefit the ordinary citizen.[30]

It would appear that despite criticisms levelled at the statistics illustrating the effectiveness of CCTV and the fears surrounding its use, the implementation and operation of CCTV will continue to increase. It has been reported that over 500 new systems are installed each week in the UK and this trend will continue. Developments in technology will undoubtedly have repercussions for policing. One commentator has claimed that 'police work is changing. We are evolving towards techno-policing with a tendency to the application of military technology'.[31]

Rapid advances in surveillance technology include the development of digital microcameras and facial recognition technology. Cameras on microchips of less than 100 square millimetres can link to facial images. The capacity for storing and transmitting information are continuing to increase and cameras can now operate over large geographical areas. These systems can then be programmed using digital computer algorithms which can alert the camera to any 'unusual' activity.[32] In the United States the development of 'electronic ankle transponders' enables the police or probation officers to track convicted offenders (usually of 'low level' crime such as shoplifting) via devices which emit silent alarms in the CCTV control rooms of shopping centres. The monitoring capability of the police is significantly enhanced by the use of such technology.

4. Conclusion

The use of technology within police forces is obviously not without controversy but it appears that police use of technology is on the increase. The police now have use of technology which permits surveillance, identifi-

[30] Honess & Chapman, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Home Office Police Research Group, Crime Prevention Unit Series (1992), Paper 35.

[31] Detlef Nogala, University of Hamburg, 'Techno-Policing: From Specialization to Common Use', *Advanced Surveillance Technologies Conference*, 4 September 1995, Copenhagen, Denmark.

[32] For further discussion see Norris, Moran & Armstrong, *Algorithmic Surveillance: The Future of Automated Visual Surveillance* (Mimeo 1996).

cation, detection, enhanced information processing, communication etc. Technology is increasingly being viewed as one of the cornerstones of an efficient police service and police crime prevention strategy. The benefits of computerisation for policing are commonly accepted as providing increased efficiency both in administrative and operational terms, faster incident access, enhanced speed of despatch and the provision of archive information. Recently the retiring Scottish Chief Inspector of Constabulary was reported as having claimed that crime fighting applications have helped improve crime detection rates in Scotland during the last few years.[33] In his Annual Report to Chief Constables he stated that IT systems were essential for effective policing. Figures published by the Scottish Office showed an increase in detection rates from 31% in 1991 to 39% in 1995/96. The systems in use in Scotland include databases where all incoming data is hosted in order to let officers know what stage an investigation is at and also to enable the analysis of the information in order to identify patterns in crimes etc. This in turn facilitates a more rapid identification of suspects and saves time and money regarding police investigations.

Despite that fact that computerisation has been applauded it has not been without its difficulties. Recently the Home Office has been criticized by one of the UK's top policemen for delays regarding the implementation of 'Phoenix'. The English Chief Inspector of Constabulary in his Annual Report slammed many of the UK forces for not having a comprehensive IT strategy despite the 1994 National Strategy for Police Information Systems. On a more positive note he commended the developments already underway such as enhancements for Phoenix in the form of Quest, a search facility regarding all convicted offenders, a national automated fingerprint identification system and HOLMES 2. In his view IT developments are crucial for the police services in order to facilitate and enhance the investigation of crime.[34]

It is apparent that that there has been a growing awareness and enthusiasm for IT within both policing. In the context of policing it appears that technology is increasingly recognized as being a valuable and innovative addition to policing. Both within the UK and the USA computerisation has achieved a wide acceptability. The difficulties in attempting to harmonize forces in line with the UK National Strategy stem from internal reluctance within local forces to succumb to influence from other forces. There is a strong sense of independence and individuality within local forces and political differences may also dictate a lack of standardisation.

However, despite internal resistance there seems to general agreement that the police need to exploit IT better to help officers in their work. The

[33] *Computing*, September 1996.
[34] Chief Inspector of Constabulary, Annual Report, 1996.

benefits of adopting a comprehensive IT strategy are manifold; IT can reduce the administrative workload, speed up response times and contribute to more efficient allocation of resources. It has been reported that 'the imposition of a national IT strategy ... will mean many forces having to adapt long-established working practices to the demands of modern technology'.[35] The implication is clear, 150 years of culture in local forces will necessarily have to change in order to accommodate the new technologies. For example, in the context of surveillance it is arguable that the introduction of CCTV will have an effect on police officer discretion. Within the criminal justice system police officers do not merely apply the law, they also exercise their discretion by considering varying factors such as the precise circumstances surrounding the offence. No two incidents are likely to be the same and as such an element of discretion exists in appraising any given situation. The concern regarding the use of CCTV is that crime detection and enforcement will become more 'automatic' with the element of discretion largely removed from the officer on the beat and transferred to the operator manning the camera system. This may, on the one hand aid the apprehension of criminals and reduce crime statistics but, on the other, it gives rise to fears of 'overzealous' policing with sanctions applying to relatively petty instances. The element of discretion affords the police officer legitimacy and promotes the notion of fairness and justice which in turn enhances police community relations.

The old image of the 'bobby on the beat' is waning and as we approach the twenty first century images of 'technocops' proliferate and undoubtedly police computer-power will continue to grow at a dramatic rate.

[35] *Computing*, April 1997.