ISSN 1758-8405

Current Criminal Law

THOMSON REUTERS

Contents -

PUBLISHED BY SALLY RAMAGE
COPEHALE, COPPENHALL, STAFFORD,
UNITED KINGDOM
TEL 01785 - 211370
FAX 01785 - 228281
WWW.SALLYRAMAGE.NET

Police Interception of Communications in the United Kingdom

Sally Ramage[1]

Police Interception Warrants

In the UK, interception of communications is principally regulated by a statute known as the Regulation of Investigatory Powers Act 2000. Only the heads of law enforcement or security agencies, or their representatives, are eligible to apply for interception warrants. These warrants are issued by the Secretary of State. Warrant applications must meet the tests of necessity and proportionality. The effective period for all new warrants is the same, but may vary after renewal, depending on their purposes. Intercepted materials are not admissible as evidence in legal proceedings, except in limited circumstances.

The Interception of Communications Commissioner

The use of interception powers is monitored by the Interception of Communications Commissioner whose annual reports to the Prime Minister are tabled in Parliament and then made available to the public. Covert investigation is permissible in the United Kingdom. Covert investigation is sometimes the only realistic means of prosecuting drug dealers, for instance. Covert investigation can provide useful supporting evidence or intelligence. When evidence cannot be secured by normal overt means, covert investigation needs to be used. Agencies other than the police can gather covert evidence and RIPA (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 (SI 2003/3171) but are restricted to the sole purpose of preventing and detecting crime. There can also be covert surveillance of computers, this being interference with property and be intrusive, requiring prior approval and a warrant to look at live e-mails. In the case NTL group ltd v ipswich crown court[2].

Statutory Parliamentary Committee

The expenditure, administration and policies relating to interceptions for national security purposes are monitored by a statutory parliamentary committee.

Investigatory Powers Tribunal

Members of the public can lodge complaints with the Investigatory Powers Tribunal. This tribunal has power to cancel warrants and award compensation. A significant decision of the tribunal is C *v. Secretary of State for the Home Department* (IPT/03/32/H, 14 November 2006).

Legislative amendments to RIPA shifted interception powers away from privacy

In recent years, legislative amendments have been introduced to enhance the implementation of the interception law and combat to terrorism. The powers to investigate post, telegraphy, telephony, telecommunications, oral communications and traffic data shows that the balance between criminal investigation and privacy has shifted towards law

[1] Sally Ramage is Annotator of the Policing and Crime Act 2009 and the Crime and Security Act 2010 in the series *Current Law Statutes Annotated*, Sweet & Maxwell, Thomson Reuters, United Kingdom.
[2] [2002] EWHC 1585.

enforcement. As such, privacy has become a secondary rather than a primary factor in legislative practice. Academic papers have long tolled the death of privacy (see, e.g., Garfinkel 1999; Sykes 1999; Whitaker 1999; Froomkin 2000). In the UK, interception of communications conducted by the government has been a long established and publicly known practice. There was no overall statutory framework governing the practice of interception in the UK before1985[3] and since that time. Regulation has in part been by provisions in various ordinances, and with obscure legal basis because the power was vested in the Secretary of State to authorise, by warrant, the interception of postal and telegraphic communications. This meant that the power to intercept was subject to executive control instead of statutory regulation and it was not until 1985 that the UK government indicated its intention to introduce legislation on interception of communications.

Interception law in the United States of America

In the United States of America, the importance of wiretap law to enforcing privacy rights lies in the precedent caselaw of *Olmstead v. U. S.* [4] *This* was a United States Supreme Court decision which held that police officials do not need a warrant to observe an individual's property from public airspace. Although the surveillance in this case was narrowly circumscribed and should have been authorised in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance. The U.S. Supreme Court allowed, without the need for a Search Warrant, a wiretap[5] of telephone calls from a private home. Since the 1960s United States' wiretaps by federal and state officials have been subject to constitutional scrutiny where there is a reasonable expectation of privacy. Wiretap Report of the Administrative Office of the United States Courts indicates that almost all 50 U.S. states have laws permitting the issuance of interception orders. In the US, interception of communications is mainly regulated by three statutes. *Title III of the Omnibus Safe Streets and Crime Control Act 1968 (Title III)* regulates interception of the contents of communications for law enforcement purposes.

The U.S. Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 (FISA) regulates interception of the contents of communications of foreign powers and their agents within the US. The Pen Registers and Trap and Trace Devices chapter of *Title 18 (the Pen/Trap statute)* regulates interception of non-content information of communications. Interception orders under the three U.S. statutes are all issued by judges. Under Title III and FISA, court order applications must be authorised or approved by high-level judicial officials, and the issue of court orders must meet the 'probable cause' test. The Pen/Trap regulatory system is less demanding, under which a court order is issued as long as the information to be intercepted is relevant to criminal investigation. The effective period for FISA orders is the longest, and Title III orders the shortest. Evidence gathered lawfully may be used in legal proceedings. The head of the Department of Justice is required by all three interception statutes to submit annual reports to Congress, but the information disclosed is different among them. Intercepting agencies are accountable to parliamentary committees. After the '9/11' terrorist attack by dring aerpoplanes into the World Trade Centre in New Youk,

[3] Between 1957 and 1981, the UK government had three official reports made available to the public, namely the 1957 Birkett Report, the 1980 White Paper and the 1981 Diplock Report. These reports provided a review of the procedures, safeguards and monitoring arrangements relating to interception of communications, but none of them recommended a single legal framework to cover all interception matters.

[4] 277 U.S. 438 [1928].

[5] The term 'wiretap' means 'telephone tapping or monitoring of telephone and Internet conversations by a third party, often by covert means.

significant amendments to the three interception statutes have been made by the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act to increase the government's interception powers.

Criminal interception by fraudsters, terrorists and for malice

The tension between criminal investigation and privacy is a hot topic, particularly after the terrorist attacks in the USA on 11 September 2001. There has always been a balancing act between privacy and law enforcement though. This tension is worsened by society's demand today for a society that is totally free from risks, result ing in a raft of legislative measures in many countries that target terrorism, some of which are the US Patriot Act, the Canadian Anti-Terrorism Act, the German Terrorismusbeka¨mpfungsgesetz, the French Loi relative a` la se´curite´ quotidienne and the UK Anti-terrorism, Crime and Security Act. All this legislation contains measures that make it easier for law enforcement authorities to investigate crime. For example, the French law requires telecom operators to store traffic data for a period of one year – regardless of indications of terrorist or criminal activities. There is a Framework Decision requiring EU member states to implement a retention measure for at least a year.

The U.K.Terrorism Act 2000 made the threat of or use of computer interception a potential act of terrorism. The use or threat of an action designed to seriously interfere with or to seriously disrupt an electronic system will be a terrorist action only if both of the following conditions are satisfied: (a) it is designed to influence the government or to intimidate the public or a section of the public, and (b) it is made for the purpose of advancing a political, religious or ideological cause.

When interception is activated by malicious ex-employees, or rogue governments, or serious organised gangs, the devastation caused can be hugely detremental to government, business, private individuals and ultimately, to economies. For instance, A U.S. cyber-terrorist attacked his employers system and the former UBS PaineWebber employee was sentenced to eight years in prison in December 2006 for planting a computer 'logic bomb' on company networks and betting its stock would go down. The disgruntled employee had left his job as a systems administrator in February 2002 after expressing dissatisfaction about his salary and bonuses,. He then planted malicious computer code in an estimated 1,000 of PaineWebber's approximately 1,500 networked computers in branch offices. This logic bomb was set to activate on 4 March 2002 and on schedule it detonated and deleted business files.[6]

An extremely serious criminal offence has been downplayed and the suspect's extradition application highlighted instead. Gary McKinnon is accused of intercepting 97 United States military and NASA computers over a 13-month period between February 2001 and March 2002. The computer networks he intercepted include networks owned by NASA, the United States Army, the United States Navy, the United States Department of Defence; the United States Department of Defence (Homeland Security), and the United States Air Force. There are utterly serious offences against a very senior nation state. McKinnon deleted critical files from operating systems, which shut down the U.S. Army's Military District of Washington network of 2,000 computers for 24 hours. McKinnon also deleted U.S. Navy Weapons logs, rendering a naval base's network of 300 computers inoperable after the September 11th terrorist attacks. McKinnon is also accused of copying data, account files and passwords onto his own computer. U.S. authorities estimate the

[6] Source: Reuters 14.12.06.

cost of tracking and correcting the problems caused by McKinnon's terrorist actions as being a sum of $700,000.

Online banking fraud is a big problem in the U.K. and increased by 90% to £23.2 million from 2004 to 2005, triggering an investigation by the House of Lords into how banks can safeguard customers' money. The House of Lords Science and Technology Committee also investigated personal Internet security, hearing evidence from representatives of APACS, the UK payments Association, and the credit card company Visa. The written evidence from ACPAS suggested that the number of phishing incidents rose by 8,000% between January 2005 and September 2006 alone. The Internet Service Providers have difficulty in keeping up with the criminal acts. Coupled with this, there has been a spate of serious activist disruption of businesses and government agencies throughout the world. Every month, there is news of another IT system being illegally intercepted. RSA, Epsilon, Sony, now Citibank all suffered high-profile breaches. When an organisation's system is intercepted, the cost of remediating the breach is very high. Prevention of such interception is important. The size of a typical enterprise IT environment is large, complex and has dozens of different platforms, multiple business partners, and hundreds or thousands of different network pathways.
In 2011, a group calling themselves *Lulz Security* has admitted responsibility for taking offline the government agency website of the UK Serious Organised Crime agency ('SOCA'). This was a denial of service (DDoS) interception. LutzSec internet criminal activity exposes the weaknesses in the online security systems and stretches cybercrime policing to full capacity.

Surveillance control by German executive- not statute
Regarding Germany's use of surveillance devices, German executive authorities have control of interception of communication**,** despite the German breach of privacy caselaw of *Klass v Federal Republic of Germany.*[7] In this case, the Court stressed that any such interference had to be justified in accordance with law and that the executive authorities should be subject to effective control, normally through the judiciary.
The decision of *Klass v. Germany* was applied to the case *Malone v. U.K*[8] where the Court found that the U.K. law on telephone tapping did not satisfy article 8(2) exception of the 1950 European Convention on Human Rights because it was not publicly accessible and did not indicate with sufficient certainty the scope and manner of exercise of discretion conferred on the relevant authorities. [9]

UK Computer Misuse Act 1990 amended by Police and Justice Act 2006
The Computer Misuse Act introduced three offences into UK criminal law; the unauthorised access to computer material; uunauthorised access with intent to commit a further offence and unauthorised modification. The offence of unauthorised access to computer material is covered by section 1 of the Computer Misuse Act 1990. For the offence to occur the access to the computer material has to be unauthorised and the individual gaining access has to be aware that his access is unauthorised. There is no requirement for the intent to be directed at a specific program or file. It is enough to prove

[7] [1978] 2 EHRR 214.
[8] [1984] 7 EHRR 14.
[9] This is the exception to the right to respect for private and family life, home and correspondence and 8(2) states : '*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

that the access was unauthorised. There is no definition of 'computer material' within the Act, enabling the Act to be applied to new pieces of technology as and when they are developed. The definition of 'computer' is 'any device for storing and processing information'. Anyone guilty of an offence under section 1 of the Computer Misuse Act will have further criminal sanctions imposed on him if this is done with the intention to commit or facilitate the commission of further offences as per section 2 of the Computer Misuse Act. A modification is a change, which impairs the operation of a computer, prevents, hinders access to a program or data or the operation of the program or data, or affects its reliability. These offences under the Computer Misuse Act are criminal offences, and on indictment and conviction, the maximum penalty is six months imprisonment and a £2,000 fine.

Interception of other telephonic communication

In the case of *Halford v United Kingdom* [10] the European Court of Human Rights in Brussells it held that telephone calls made from business premises were covered by the notion of 'private life' as protected under article 8 ECHR and that employees who made calls on internal systems had a reasonable expectation of privacy. Another such case went to Brussells from Switzerland, *Amman v. Switzerland* [11] and the court held that the tapping of the applicant's telephone conversation amounted to a violation of article 8, ECHR (which applied to interference executed on business premises) of Switzerland because the national law was not sufficiently clear to clarify the scope and conditions of the authorities' discretionary powers in this area. Amman's prosecution was as a result of a conversation which the government had intercepted, as a result of which Amman's personal information was placed on a national register.

English Police covert interception on police premises

The case of *PG and JH v. United Kingdom*[12] was due to the use in a criminal prosecution case of police covert interception as evidence in subsequent criminal proceedings. The European Court held that the protection of article 8 applied to recording devices operated without the knowledge and consent of the individual on police premises. The European Court noted that the police lacked the statutory power to carry this out and found a violation of article 8. However they found that these measures were justified under article 8(2). In r v Sutherland, proceedings were stayed because the police acted in bad faith. (See *R v Mason*)[13]

UK Regulation of Investigatory Powers Act

It was the decision in the case of *Khan v. United Kingdom*[14] that caused the UK government to draft and enact the statute titled Regulation of Investigatory Powers Act ('RIPA'). *Khan* was a case of the use of unregulated interception devices resulting in an unjustified interference with the Khan's private life and correspondence under article 8. There are safeguards that unlawfully obtained evidence must not be admissible if it seriously prejudiced the applicant's right to a fair trial and so the court took the view of the overall fairness of the trial rather than prescriptively, deciding that although article 8 was breached, article 6 was not. Since IOCA was enacted, there have been enormous changes in telecommunications technology and communications services, such as the mounting popularity of mobile phones and communications via the Internet, the expansion of non-

[10] [1997] 24 EHRR 52.
[11] [2000] 30 EHRR 843.
[12] The Times, October 19, 2001.
[13] [2002] 2 Cr App R 38.
[14] [2000] 31 EHRR 45.

public telecommunications networks, and the surge in the number of private companies offering parcel and document delivery services. These changes have given rise to new human rights concerns and gone beyond the scope of IOCA. As such, the UK government recognized the need for new legislation as portrayed in a consultation paper published in 1999. A year later, IOCA was repealed and replaced by the Regulation of Investigatory Powers Act 2000 (RIPA), which has become the primary legislation regulating interception of communications in the UK. However, anti-terrorism measures are not the only ones that favour criminal investigation to the detriment of privacy. Many recent laws have been passed that facilitate law enforcement, particularly in the context of information and communications technologies (ICT). The UK Regulation of Investigatory Powers Act 2005 contains far-reaching powers on telecommunications interception and a decryption order.

When surveillance termed intrusive surveillance is deployed, there must be an intrusive saurveillance authority. Only the Metropolitan Police Service; City of London Police; Police Service of Northern Ireland; Ministry of Defence Police; British Transport Police; SOCA; Army; Navy; Royal Air Force;; HMRC; Office of Fair Trading; MI5; MI6; GCHQ; any npolice force under s.2 Police Act 1996; any police force under and s.1 Police (Scotland) Act 1967 can conduct directed surveillance.

Disadvantages of RIPA

There are commercial disadvantages caused by such legislation, examples of which is restrictions on the use of cryptography which make police computer searches easier but also weaken e-commerce and create more fraud (Koops 1999) Sweeping investigation powers to the detriment of privacy with the aim of strengthening security by way of more legislation may tip the balance between criminal investigation and privacy towards law enforcement and have bad long-term effects on society as well as the short-term good effect of increased security.

Developments in communications technologies

For a better understanding of historical developments in the various investigation powers that target different forms of tele-communications, it is useful to have some insight into the general history of communication technologies. The oldest means of telecommunications is the post .Then the automation of telegraphy or telex led to the possibility of ‘home telegraphy in the 1930s. Attempts to send images across a distance became successful in the 1920s, when newspapers and press agencies started transmitting photographs. In the 1970s, these facsimile machines gained wider popularity. Another development was the invention of mobile telephones. The use of mobile telephony has exploded. But the most significant telecommunications development of the past decades is the Internet. In the 1990s, the courts allowed the power of requesting traffic data to also include future traffic data; this allowed police to examine traffic data more systematically, since previously they had to rely on the data that happened to be stored with the Telecommunications company at the time they requested traffic data. Twentieth-century communications technologies – telephone, facsimile, electronic mail – could at first be used without the possibility of judicial investigation; the introduction of investigation powers to intercept telecommunications therefore constituted an investigation shift. Intercepting telecommunications in transport is traditionally only allowed for communications by the suspect; for stored telecommunications, there is no such requirement: The police can investigate stored communications of non-suspects. In wiretaps, the object has been broadened from conversations to include all forms of telecommunications; in traffic data investigation, the object has been extended to include future communications, as well as location data and website-viewing information, but it

has eventually also been narrowed by excluding information on the contents of communications.

In the United Kingdom, police and other state authorities employ a variety of techniques to gain information in the prevention or detection of crime, many of which intrude into the individual's private life. In particular, there is employment of covert surveillance techniques such as telephone tapping, bugging, and the use of closed circuit television surveillance, carried out without the individual's knowledge. The disadvantage of using covert means is that there are consequences to decisions made using incorrect or inaccurate information. Another disadvantage is the prospect of a leak of that information. Yet, the importance of covert investigation is that it produces incontrovertible evidence. Intrusive surveillance under s.26 (3) RIPA includes covert surveillance carried out on residential premises or private vehicle; if someone is in the house or vehicle or the use of an audio or visual device. The Chief Constable or Commissioner must authorise the intrusive surveillance. The authorising officer must state explicitly what is being authorised; and who-by name- is the suspect.

Cyber terrorism

In the UK, 2006 saw very little of security scares such as major virus outbreaks but there has been a growing awareness of threats to our personal and corporate data, whilst 2005 was all about Trojans and spyware and 'phishing'5 . One example of the 2006 data thefts were from community sites such as MySpace which were targeted as they reached a critical mass, making them very tempting for the criminals to steal the information which members make available on them. The fact that they are intentionally easy to contact meant new threats grew up around these communities. Software applications appeared for sale online in 2006 which can launch attacks against whole swatches of the MySpace community. This enables greater social engineering. So for example, criminals can target anybody who has expressed a preference for a particular band or sports team or who has included other keywords in their profile, meaning attacks can be tailored to be more relevant and therefore more appealing to the unsuspecting victim. With increasing amounts of information about individuals on social networking sites, blogs or even searchable via Google more targeted forms of phishing are developing. AS for companies' data, with increasing amounts of information available on easily searchable online, attacks are becoming even more targeted. Examples of company data losses were in February 2006 when security vendor McAfee warned staff that a CD containing sensitive data on current and former employees had disappeared while in the care of an external auditor and in May 2006 when back-up giant Iron Mountain lost tapes containing employee data from one of its customers. In November three laptops were stolen from LogicaCMG containing sensitive employee data belonging to the Metropolitan Police force. One factor for such data thefts is because modern workforce is increasingly mobile and sensitive data therefore resides in more portable and easily lost or stolen devices. A recent enquiry has uncovered the number of laptops stolen from key UK government departments over the past year, raising questions and concerns about sensitive data falling into the wrong hands. The Ministry of Defence reported 21 laptops stolen between July 2005 and July 2006. The UK Home Office suffered 19 stolen laptops over the past year including four laptops stolen from the Identity and Passport Service. The UK Core Home Office unit suffered seven stolen laptops, while HM Prison Service had eight laptops stolen. The Department of Trade and Industry had 16 laptops stolen over the past year, while the Department for Work and Pensions reported it had nine laptops stolen. The Department of Health said it had lost 18 laptops. The government department Defra lost 17 laptops. Other findings, opinions and statistics which came to light over the course of 2006 suggest that UK companies are doing little to mitigate the threat of damaging data losses and still fail

failure to stop the use of removable storage devices such as iPods and digital cameras which are easily secreted on employees' persons. It is widely known that most corporate frauds, financial and otherwise, are performed by employees with inside knowledge. Cyber criminals steal billions from cash machines with the help of cameras installed on cash machines. Western banks use a very weak "bank-client" system in terms of protection. Cyber terrorists have been tapping phones of the UK military in Iraq and then called their relatives in Britain and it appears that the Western countries are not very highly concerned with the threat of cyber terrorism. Magnus Ranstorp, former Director of Centre for the Study of Terrorism and Political Violence at the University of St Andrews, Scotland, wrote an article entitled, 'Al Qaeda Wages Cyber War against US' in which he states that al-Qaeda pays much attention to studying the cyberspace and searching for vulnerable spots in it, and the question is not whether it will wage the war, but when it will do it. The American government has killed Osama Bin Laden in 2011 and it may be that much of this surveillance will now be unnecessary.

Russia

One of the major frauds in the history of world banking has been 15 years of a Russian fraud with counterfeited advice notes to 2006. It was about faked credit notes. In 1991-92, 400 billion rubles were embezzled from the Russian Central Bank. This banking theft ceased because of the joint effort of the Russian Central Bank staff and Russian Ancort Company which installed a system of cryptographic protection of notes. As a result no fake credit note now come from the Russian Central Bank. The murder by shooting in 2006 of Russia's Central Bank First Deputy Head Andrei Kozlov reminds the world of the 1990's when the Central Bank became the object of an unprecedented criminal attack known as the "fake advice notes fraud." The State Duma established a special committee to investigate criminalization of banking systems, particularly in investigating this murder. The cause of the biggest fraud in the history of world banking was due to the 1991-92 a cyber war in Russia. Management of national strategic financial resources which was partially under the control of criminal subjects. The criminal element damaged information systems, processes and critically important national resources; and undermined the political and social system. This placed psychological pressure upon the Russian population and its aim was the destabilization of society. The information war imposes false reports, listening-in and distortion of information, establishment of false points for information transmission and many other things, which now consists the gist of current high-tech information wars.The Central Bank was typical of the whole former USSR information systems of the former Soviet Union at a tactical level. Encoding of information in handwritten documents took a long time and caused army units to exchanged information by so-called talking tables, where words like 'shells' were replaced by 'water-melons' and cartridges were called 'cucumbers.' This was done manually. This 'fruit-and-vegetables' exchange of information was broadcast. Then there was a ban on the use of talking tables without encoding. This same 'fruit' coding played its role in the case with fake advice notes. Protection of financial advice notes exchanged between cash calculation centers was a tactical task for the Russian Central Bank as it was for the army. In the USSR it became apparent that a skilled cyberattack would be able to penetrate and destroy Russian information systems. Trillions of rubles were stolen, resulting in collapse of many state-financed enterprises and bankruptcy of major companies, comparable to a nuclear aggression against Russia, a real cyber war.

A unique cryptographic protection system

A unique cryptographic protection system was devised for the Central Bank of Russia in the 1990's. Some elements of the system have no analogs in the world. Each payment

under an advice note was protected by a mini electronic digital signature. The notes could be sent via telex between the cash calculation centers. It is impossible to counterfeit such payment. The technical part of this assignment was done only by Ancort Company which delivered 6,000 encoders, worked out unique cryptographic solutions for 1,800 clients of the network, developed rules of functioning of the network and many other things to secure needed level of information protection of the Central Bank network. The Central Bank financial system consisted of 1,800 calculation centers all over Russia. Each center was to communicate with the others. So, each centre was supposed to be equipped with a certain number of encoders and trained operators how to use them.
The embezzled money was taken abroad and the Russian government response to this cyber terrorism was to form thousands of encoding units in police troops and Air Forces. Cyber terrorism uses technical means to upset the administrative resources.. However, cyber terrorism is not only a Russian phenomenon as is the Al-Qaeda's cyber terrorism. Exhibitions of special equipment for interception and listening devices held in Russia in 1991-93, created outside interest which meant that interest in cyber terrorism was to attack more computer networks or internet. This cyber terrorism is the main threat of the 21st century.

No privilege exemption for United Kingdom's MP's against this Interception Act 2007

Rt. Hon. Sir Swinton Thomas, the now retired Interception of Communications Commissioner has a large section in his delayed report: Report of the Interception of Communications Commissioner for 2005-2006 which discusses the constitutional issues resulting from the 'Wilson Doctrine'. The Wilson Doctrine applies to all forms of communication, to Members of the House of Lords, and to electronic eavesdropping by the intelligence agencies. The Doctrine has remained in force ever since, and on 30 March 2006, the Prime Minister, Mr Tony Blair, said in answer to a question that the Wilson Doctrine would be maintained. It is an issue which falls squarely within the responsibilities placed on the Interception of Communications Commissioner by Parliament by Section 57 of the Regulation of Investigatory Powers Act 2000. The Doctrine may have been defensible when it was first enunciated in 1966 when there was no legislation governing interception and there was no independent oversight. In 1966 there was no requirement for a warrant with all the safeguards that are attached to that operation now. However, in 2006, the interception of communications is the primary source of intelligence in relation to serious crime and terrorism and is strictly regulated. Members of Parliament have historically developed Parliamentary Privilege, to allow them to criticise people or institutions, without the fear of prosecution for libel etc., so in that sense, they are above the law, and being seen to be above the law, is an important constitutional safeguard for non-MPs. Some MPs fear that the situation now is the same as it was in 1966 when it was at least theoretically possible for the Executive to intercept communications for its own purpose. Safeguards are in place, however.
For there to be interception, there must be a warrant in place, signed by the Secretary of State authorising the interception. The grounds for doing so are essentially national security (including terrorism) and the prevention or detection of serious crime. There is oversight by the Commissioner to prevent wrongful use. Since the Interception of Communications Commissioner only deals with intercepted data or communications traffic data at the level of authorisations, warrants and certificates, the public might be concerned as to the Commissioner's ability to personally ensure that there is no improper interception of the communications of a public figure when dealing with large scale data warehousing and data mining. The interception of communications is the most important investigative tool in the investigation of serious crime, such as fraud, drug smuggling, the

downloading of child pornography, sexual offences with minors and perjury. There are other people who may well have the equipment and knowledge to conduct electronic intercepts and communications traffic data snooping, without falling under these bits of legislation, or the Police departments of the Ministry of Defence e.g. the Special Forces Support Group or the Special Forces Reconnaissance and Surveillance Regiment. Not all interception of communications or communications traffic data snooping occurs centrally at a Communications Service Provider. It could also be done by private investigators who turn up at , say a bank, and who may be working for, the Treasury, claiming 'anti-terrorism finance investigation' or 'international trade sanctions' powers, or for the Department for Work and Pensions investigating 'benefit fraud'. **T**here is no other country in the world that provides the privilege to its elected representatives and Peers to be immune from having their communications lawfully intercepted with the accompanying advantage that they may be immune from criminal investigation and prosecution. There is no immunity from criminal investigation and prosecution for Members of the House of Commons or the House of Lords, even though Parliamentary Privilege protects them from some civil court cases. Note that the European Parliament, the National Assembly of Wales, the Scottish Parliament, were all established prior to the Regulation of Investigatory Powers Act 2000.

Interception of Communication in other countries

The German Federal Government has enacted a law that allows the use of mobile phone jammers during major events, and in prisons. Blocking the use by criminals of mobile phones is seen as an important counter-terrorism weapon. The German government enacted such disablement to prevent unauthorised calls made by prison inmates, where mobile phones are often smuggled into prisons despite heavy prison security. Some German Information Technology industry Bitkom group strongly opposed the statute, arguing that the plans were technically impraticable. To prevent calls in a soccer stadium or in a prison, the jammer would need a lot of electrical power and Bitcom claimed jamming would result in the block phone conversations in nearby neighbourhoods and cause network instability and quality.

U.S. can disable enemy satellite transmissions

The U.S. has electronic-warfare squads capable of disabling enemy satellite transmissions.The U.S. has established mobile teams equipped with electronic gear capable of disrupting attempts to interfere with its satellite resources, and its Air Force Space Command is tasked with protecting U.S. satellites from attack.

Human Rights and interception of communications

The United States 2001 Wiretap Report of the Administrative Office of the United States Courts says that forty-six jurisdictions have laws permitting the issuance of interception orders. *Katz v. United States* had already shifted the Fourth Amendment focus to 'people, not places.' Since *Katz*, the central doctrinal question for surveillance has been whether an individual has a 'reasonable expectation of privacy' in a particular communication.

Investigative technique: Electronic eavesdropping

One category of firsinvestiugative technique is where those doing the surveillance listen in to the content of the communications. Police or others might learn the content of communications by means of electronic eavesdropping, or bugging. This eavesdropping is typically accomplished by placing a listening device in or near an area where targeted conversations are likely to take place. These devices acquire the conversations in their acoustic, rather than electronic, form. The devices record the conversations or transmit

them to law enforcement personnel at a listening post or other location. The police or others can also learn the content of communications by means of wiretaps, which intercept the content during the course of electronic transmission over a radio or telephone line facility. In the U.S. the courts have applied the 'reasonable expectation of privacy standard' to bugging and wiretap to determine whether a Fourth Amendment 'search' has occurred.

Investigative technique: trap and trace device

A second category is the instance that police or others learn the 'to/from' information of communications. The term 'pen register' is used to refer to the list of telephone numbers, e-mail addresses, or similar information that receives a communication from the target of the investigation. The term 'trap-and-trace device' is used where communications are traced back to their source, such as the phone number from which a call is made. The U.S. Supreme Court has held that the Fourth Amendment does not prevent third parties from voluntarily turning over the stored records to law enforcement. In this modern world, where the content of so much sensitive personal information is held by third parties, law enforcement officials can often learn about content or to/from information from stored records rather than by intercepting a call or e-mail as it occurs.

The Fourth Amendment to the United States Constitution, is incorporated in and made applicable to the states by the Fourteenth Amendment. There are restrictions of federal statutes such as the Electronic Communications Privacy Act ('ECPA'). The Fourth Amendment was first applied to state-ordered electronic surveillance by the Supreme Court in *Berger v. New York* [1967]. Court found New York's eavesdropping statute to be constitutionally defective because it did not require a showing of probable cause before an eavesdropping order would issue, and did not require specification of the crime that had bee nor was being committed and of the particular conversations being sought.The statute authorised orders of excessive duration; and did not require orders to be promptly executed;and permitted extensions of the original eavesdropping period without a showing of probable cause; did not require termination of the eavesdropping once the conversation sought was seized; did not require a showing of 'exigency' to justify use of eavesdropping as an investigative technique; and did not require a return of the warrant.

Detailed guide to compliance of privacy protection in the U.S. case *Berger*

The *Berger* decision gave the states a detailed guide to compliance with the Fourth Amendment in their use of eavesdropping and wiretap techniques. After *Berger*, states were on notice that their surveillance statutes and practices must ensure 'adequate judicial supervision' and 'protective procedures.' Specifically, orders must be issued by a judge, upon a showing of probable cause, with specification of the crime committed or about tube committed and the conversation or conversations to be seized. Issuance of an order must be based upon a showing of circumstances that justify the use of the intrusive techniques of interception or eavesdropping. The orders must be for a limited time and subject to a requirement of prompt execution. Extensions of an order must be based upon probable cause, and the order must be returnable to the court to ensure judicial supervision of the order's execution.

U.S.Omnibus Crime Control and Safe Streets Act 1968

These constraints were codified and made more specific in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 or 'Title III' as it is generally called established substantive and procedural requirements for federal interception orders. This was followed by the Electronic Communications Privacy Act 1986, which addressed newer communications technologies such as mobile telephones and electronic mail. The ECPA

broadly prohibits all interceptions of the contents of wire, oral, and electronic communications, except where those interceptions comply with the ECPA requirements. Where interceptions will be made by law enforcement agencies, the ECPA specifies the officials who may apply for an order, the crimes or categories of crimes in connection with which an order may be sought, the probable cause showing that the applicant must make, and the findings and 'minimization' requirements that the order must contain. The ECPA also requires state and federal courts issuing interception orders to make detailed reports concerning those orders to the Administrative Office of the United States Courts. The ECPA also sets forth standards for pen register and trap-and-trace orders, and for government access to stored records held by third parties. Under the Fourth Amendment and ECPA constraints, states that wished to perform wiretaps were required to enact statutes that closely track the probable cause, minimization, and other requirements of federal law. A number of amendments and proposed amendments to state laws add computer crimes and 'terrorism' including various terrorism-related crimes, to the lists of offences for which wiretap and similar authority may be granted. These changes are consistent with the requirements of the ECPA, which permits state interception orders in connection with the offence of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offences.

U.K. absence of clear law of privacy

In the UK, there is an absence of a clear law of privacy except that which is contained in the Human Rights Act 1998. Interception of communications breaches the right to privacy and the right to privacy or the right to a private life is at the heart of individual freedom and the right to be free from arbitrary state interference. Article 8(2) of the European Convention on Human Rights stipulates that there may be no interference with the exercise of the right to a private or family life by a public authority unless the restrictions are achieving legitimate aims such as the prevention of disorder or crime or the protection of health or morals. The expression 'private life' covers privacy issues relating to access to personal information. It covers interference with privacy by surveillance techniques. 'Private life' covers the right to communicate private information with others. The right to private life, however, is a conditional right and interferences are permitted under article 8(2) ECHR, provided they meet the requirements of legitimacy and necessity. The European Court of Human Rights has been instrumental in protecting the right of correspondence, recognising the right to communicate with friends or relatives and also the right to carry on business communications. In the case *PG and JH v United Kingdom*[15] the European Court said that a member state would be afforded a good deal of discretion provided the technique of telephone tapping had a proper legal basis. The Court held that the tapping of the applicants' telephone had been carried out in the context of an investigation and trial concerning a suspected conspiracy to commit robbery and so was justified under article 8(2). Thus, was alleged illegally obtained evidence allowed to be used in subsequent criminal trials. As to surveillance and individual privacy, the Court has held that CCTV footage is a violation of the applicant's rights when footage was used in newspapers and on television programmes without sufficient safeguards to ensure his anonymity. The wiretapping case, *Malone v United Kingdom* and the bugging devices case *Khan v United Kingdom*[16] resulted in the statute Interception of Communications Act 1985

[15] The Times, October 19, 2001.
[16] [2001] 31 EHRR 45.

which put telephone tapping on a statutory basis and these provisions are now contained in the Regulation of Investigatory Powers Act 2000, under which executive use of such methods are supervised by an independent and legally qualified Interception of Communications Officer. As traffic on the 'information superhighway' continues to explode a number of substantive questions about the use and abuse of these information networks arises. One issue of primary concern is whether the current law provides adequate protection for the individual's right to privacy in the workplace from threats posed by computer technology, electronic eavesdropping, video and sound recording equipment, and databases filled with personal information. What are the ramifications for an employees' right to privacy in the workplace? Does an employer have the right to search an employee's computer files or review the employee's electronic mail ("E-mail")?

The right to privacy

Privacy has taken on multifarious meanings so that it no longer conveys one coherent concept. Privacy rights, guaranteeing an individual's right to a private life, find their authority in the UK Human Rights Act 1998. Privacy is broadly defined privacy as the right of the individual to control the dissemination of information about oneself. The difference between Human Rights privacy and the tort against privacy is that the type of protection provided to individuals in human rights protects against governmental intrusion while tort law primarily protects against invasion by private parties.

Cameraphones: Innocuous Gadgets or Workplace Threats

Employers have become wary of these fun little devices because they have the potential to create big privacy problems on the job. On employees' use of camera-phones is a problem and more employers are realizing the need for a formal policy that puts employees on notice as to the limits of permissible camera-phone use in the workplace. Inappropriate use of camera-phones can violate myriad laws already on the statute books. An employee whose picture is taken in a work location where privacy is reasonably expected (e.g., a company changing room or restroom) can assert a cause of action tort law. Photos of employee meetings can violate company policy, which prohibits employer surveillance that might cool union activity. Intellectual property and unfair competition laws prohibit photographic theft of trade secrets. Because of their small size and easily hidden camera function, camera-phones are obvious potential tools for corporate espionage; a camera-phone user can secretly snap a picture of any part of a Research &Development process and just walk away. In the hands of dishonest employees, camera-phones can also lead to fraud through the covert photographing of customers' credit cards and identification documents. Finally, a disgruntled employee can use a camera-phone to fabricate evidence to support a claim of unlawful harassment or a violation of workplace health and safety rules. A Member of Parliament was removed from the House of Commons after he was caught using the device. The single most important thing an employer can do is create and consistently follow a camera-phone policy. As with all employment policies, this serves two purposes: it puts employees on notice of the limits of permissible camera-phone use in the workplace and prevents employees who are disciplined from claiming that they were singled out for retaliatory, discriminatory or other unlawful reasons.

A written camera-phone policy in the workplace

Companies should distribute the written policy to employees periodically and require employees to acknowledge in writing that they have received and understood the policy. Short training sessions for managers charged with enforcing the guidelines are necessary. An effective policy should: strictly prohibit the taking of photographs and videos—whether by camera-phone or any other device—in areas such as restrooms, locker rooms

and other facilities where employees have a reasonable expectation of privacy; require employees to obtain written permission before taking or distributing any photographs, videos or recordings of any type in the workplace; reiterate employees' existing nondisclosure and confidentiality obligations; and state the consequences for violation of the policy (e.g., employer confiscation of the camera-phone, 'appropriate disciplinary measures, up to and including termination of employment' and the employer's intent to seek any available means of legal redress) . Beyond these measures, the guidelines depend on the organization's specific needs and structure. The most extreme option is to ban camera-phones on company premises altogether, as do automotive giants DaimlerChrysler and BMW and—ironically—camera-phone manufacturer Samsung. A more permissive option, adopted by General Motors, is to require employees and visitors to surrender camera-phones only before entering Research and Development areas and other sensitive locations. A third option is to require employees to disable the camera function in the workplace, as Texas Instruments does. Whichever option is chosen, constant and uniform enforcement is critical. A strong policy is vital because the devices now constitute more than 4 percent of worldwide cell phone sales. Today, most cell phones are equipped with cameras. The potential usefulness of camera-phones in the workplace will continue to grow as technological improvements lead to improved photograph resolution. The positive aspect of camera phones is that they can increase workers' productivity. The small size of the devices and their ability to take and send digital photographs (and in some cases, videos) instantly over the Internet have the potential to increase employee productivity. A salesperson could, on the spur of the moment, showcase her products to a potential buyer, eliminating the need to schedule a formal sales call or to carry heavy products to show the potential customer. Many estate agents, in the U.S and the U.K. provide a virtual tour without requiring a client to leave home.

Electronic privacy in the workplace

Regarding electronic privacy in the workplace the case of Arias *v. Mutual Central Alarm Services, Inc.*[17] The former employees claimed that the company illegally recorded and listened to their private telephone conversations in the work place. The company monitors all ingoing and outgoing telephone calls as part of its security service to its clients. The court denied summary judgment to the company, finding that there was a fact issue regarding whether the interceptions were made within the ordinary course of business, thereby exempting the company from the ECPA Act. So, in *Sanders*, excessive and continuous interception was found to be a violation of the Act because there was no legitimate business reason for such drastic measures. As in *Arias*, a fact question will be found to exist where the legitimate business concern is not clear cut.

Knowledge of employer's monitoring is not prior consent

In *Watkins v. L.M. Berry & Co*[18] the court found that an employee's knowledge of her employer's capability to monitor private telephone calls was not prior consent under the Act. This case makes it clear that every employer should get its employee's informed consent to monitor electronic communications before doing so.

Reasonable expectation of privacy

The case of *Bohach v. City of Reno*[19] addresses the question of whether the plaintiffs had a

[17] S.D. N.Y., No. 96 Civ. 8447 (LAK and 96 Civ. 8448 (LAK), Sept. 11, 1998).
[18] 704 F. 2d 577 (11th Cir. 1983).
[19] 932 F.Supp. 1232 (D.Nev. 1996).

reasonable expectation of privacy in the use of a computer message board at their workplace under the fourth amendment. When the message system was installed, a memorandum was sent to all users notifying them that their messages would be logged on the network and that certain types of messages were banned. The court agreed with the defendant employer that the employees' expectation of privacy was diminished.

Monitoring an employee's telephone calls

Can an employer monitor the telephone calls of an employee, who the employer believes is revealing confidential company trade secrets? There are numerous United States court decisions addressing this and they can help us in the UK to understand this Bill. Some of these court decisions find the 'business extension' exception applicable and other decisions do not. In *James v. Newspaper Agency Corp*[20] the employer had monitoring equipment installed by the telephone company, and it informed its employees in writing that phone calls in certain departments (particularly those dealing with the public) would be monitored, both for quality control purposes and as some protection for employees from abusive calls. The 10th Circuit noted that the monitoring was not done surreptitiously, and ruled in favour of the employer, concluding that the business extension exception applied. In *Simmons v. Southwestern Bell Telephone Co*[21] the employer had a written policy that certain specified telephone lines would be monitored for quality control of its employees. Additionally, the employer prohibited personal calls on those lines. An employee sued when he learned that his personal calls on these telephone lines had been monitored. The court ruled that the employer monitored these telephone lines in the ordinary course of business, and in so doing, the Court relied on defendant's policy against the use of these phones for personal calls. The Court emphasized that the employee had been warned about making personal calls on these lines and knew of other lines in the office that were not monitored. The Court concluded that the employer had a legitimate business interest and the continuous monitoring of these lines for quality control purposes was upheld. Similar to the *Simmon's* case is the 5th Circuit in *Briggs v. American Air Filter Co., Inc* [22] held for the employer where it found that an employee's supervisor had particular suspicions that the employee was disclosing confidential information to a business competitor, had warned the employee not to disclose such information, and knew that a particular telephone call was with an agent of the competitor. The court held that it was within the "course of business" for the supervisor to listen to the conversation on an extension phone as long as the call involved the type of information he feared was being disclosed and the extension telephone extension used to monitor the call was made with interception equipment furnished to the employer by a communication services provider. In *Watkins v. L.M. Berry & Co*[23] the employer had a policy of monitoring employees' sales calls. The employees were advised that their personal calls would not be monitored except to the extent necessary to determine that the call was of a personal nature. The employee sued when he discovered that the employer had monitored a call in which the employee discussed a job interview with a perspective employer. The court found that the interception was not in the ordinary course of the employer's business. The Court relied principally on the fact that the employee was an at-will employee and the employer had no legal interest in his future employment plans. The Court stressed that the term 'in the ordinary course of business' cannot be extended to mean anything about which an employer is curious. The Court concluded that personal calls could not be intercepted in the ordinary course of business under the employers stated policy, except to the extent

[20] 591 F. 2d 579 (10th Cir. 1979).
[21] 452 F. Supp. 392 (W.D. Okla. 1978).
[22] F. 2d. 414 (5th Cir. 1980).
[23] 704 F.2d 577 (11th Cir. 1983).

necessary to determine whether the call was personal or not. The Court distinguished this case from the holding in the *Simmons* case. In *Deal v. Spears*[24] the 8th Circuit held that the employer violated the statute by tape recording and listening to all calls, including personal calls, even though the employer's suspicions of theft were a valid reason to monitor calls to the extent necessary to determine their nature.[25] Here, the court did not uphold an employer's right to intercept employees' telephone calls under the 'business extension' exception when it found the employer purchased a recorder at Radio Shack, privately connected the recorder to an extension phone line to automatically record all conversations. Since the recorder installed did not qualify as normal telephone equipment, the exclusion to the Act did not apply. In *Williams v. Poulos*[26] the 1st Circuit determined that a custom-made monitoring system consisting of 'alligator clips attached to a microphone cable at one end' and an interface connecting a microphone cable to a VCR and video camera on the other cannot be considered telephone equipment. In *Sanders v. Robert Bosch Corp*[27] the 4th Circuit found that a reel-to-reel tape recorder that continuously recorded certain telephone lines did not qualify for the exclusion, since it did not further the plant's communication system. In *Pascale v. Carolina Freight Carriers Corp* [28] the District Court in New Jersey held that tape recorders that the employer installed to intercept employees' telephone conversations were not "telephone instruments or equipment" for purposes of the 'business extension' exception under the Act. Citing *Poulos* and *Sanders,* the District Court found that the tape recorders did not further the employer's communications system in that they did not have a positive impact on efficiency, clarity, or cost of the system.

Privacy rights and covert police interception of communications

Revisiting *R v Khan* and examining the issue of interception of communications as a privacy issue is important. Khan had arrived from Pakistan at Manchester airport on the same flight as his cousin Nawab. When stopped and searched, Nawab was found to be in possession of heroin with a very high street value. He was interviewed, arrested and charged. No drugs were found on Khan who made no admissions on interview and was released without charge. Later Khan was in Sheffield, at the home of a man named Bashforth. Police installed a listening device outside. Neither Khan not Bashforth was aware of its presence. The police obtained a tape recording of a conversation. In the course of the conversation, Khan made statements which amounted to an admission that he was a party to the importation of drugs by Nawab. He was arrested and jointly charged with Nawab. The judge admitted the intercept evidence and Khan was rearraigned and pleaded guilty to being knowingly concerned in the fraudulent evasion of the prohibition on the importation of heroin. The Court of Appeal dismissed his appeal. *R v Khan* raised issues of whether the evidence was admissible and if admissible, whether it should have been excluded by the judge in the exercise of his discretion under common law or under section78 of the Police and Criminal Evidence Act 1984. [29] At that time, there was no

[24] 980 f.2d. 1153 (8th Cir. 1992).

[25] The 'business extension'exclusion requires that the monitoring equipment used to monitor telephone calls be standard telephone related equipment supplied by the service provider for connection to the phone system. Recent decisions have excluded phone monitoring equipment that was not normal telephone equipment neither obtained, nor installed by a standard service provider.

[26] 11 F.3d 271 (4th Cir. 1994).

[27] 38 F. 3d 736 (4th Cir. 1994).

[28] 898 F.Supp. 276 (D.N.J. 1995).

[29] Section 78 PACE states: ''In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it. Nothing in this section shall prejudice any rule of law requiring a court to exclude evidence. This section shall not apply in the case of proceedings before a magistrates' court inquiring into an offence as examining justices.'

legal framework regulating the installation and use by the police of covert listening devices. In the light of *R v Sang,* the argument that the evidence of the taped conversation was inadmissible could only be sustained if two wholly new principles were formulated: the first would be that Khan enjoyed a right of privacy in respect of the taped conversation; the second that evidence of the conversation obtained in breach of that right was inadmissible. There was no such right of privacy in English law, and even if there were, evidence obtained improperly or even unlawfully remains admissible, subject to the judge's power to exclude it at his discretion. If the circumstances in which the evidence was obtained amounted to an apparent invasion of Khan's rights of privacy under article 8, that was accordingly something to which the court must have regard. The sole reason why the case went to the House of Lords was the then lack of a statutory system regulating the use of surveillance devices by the police. Privacy is a sweeping concept, encompassing freedom of thought, control over one's body, and solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. What must be borne in mind when thinking about the meaning of privacy is that when we protect privacy, we protect against disruptions to certain practices. A privacy invasion interferes with the integrity of certain practices and even destroys or inhibits such practices. Privacy is a general term that refers to the practices we want to protect and to the protections against disruptions to these practices. Privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the practice of which it is a part. What does it mean when we say that these aspects of life are private? Many recognize the importance privacy for freedom, democracy, social welfare, individual well-being, and other ends. Many also assert ithat t is worth protecting at significant cost. Society's commitment to privacy often entails restraining or even sacrificing interests of substantial importance, such as freedom of speech and press, efficient law enforcement and access to information. The use of the word privacy constitutes the ways in which we employ the word in everyday life and the things we are referring to when we speak of privacy. The word privacy is currently used to describe a myriad of different things:- freedom of thought, control over personal information, freedom from surveillance, protection of one's reputation, protection from invasions into one's home, the ability to prevent disclosure of facts about oneself, and an almost endless series of other things.

The U.K. has no privacy law

As the UK has no privacy law, an examination of U.S. caselaw reveals their treatment of privacy. In *Olmstead v. United States* the Court held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespass into the home. However in 1967 the Court changed its view in *Katz v. United State,* holding that the Fourth Amendment *did* apply to wiretapping. In *California v. Greenwood,* the Court held there is no reasonable expectation of privacy in garbage because it is knowingly exposed to the public. In Florida *v. Riley,* the Court held that the Fourth Amendment did not apply to surveillance of a person's property from an aircraft flying in navigable airspace because the surveillance was conducted from a public vantage point.

Second Party also has rights

The fact that the tape recording in *R v Khan* was between two persons can illustrate that privacy cannot be pleaded since a person other than Khan had rights to the conversation, as illustrated by the US case, *Haynes v. Alfred A. Knopf, Inc.* The *Haynes* case involved

Nicholas Lemann's book about the social and political history of African Americans who migrated from the South to northern cities. The book chronicled the life of Ruby Lee Daniels, who suffered greatly from her former husband Luther Haynes's alcoholism, selfishness, and irresponsible conduct. Haynes sued the author and the publisher under the public disclosure of private facts tort, claiming that he had long since turned his life around and that the disclosure of his past destroyed the new life he had worked so hard to construct. Judge Posner, writing for the panel, concluded that there could be no liability for invasion of privacy because a person does not have a legally protected right to a reputation based on the concealment of the truth and because the book narrated a story not only of legitimate but of transcendent public interest. Although it did not hinge on the shared nature of the information, this case illustrates that personal information rarely belongs to just one individual; it is often formed in relationships with others. Ruby Daniels's story was deeply interwoven with Haynes's story. Daniels had a right to speak about her own past, to have her story told. This was her life story, not just Luther Haynes's. As early as 1891, the US Court articulated this concept in *Union Pacific Railway Co. v. Botsford.* In holding that a court could not compel a plaintiff in a civil action to submit to a surgical examination, the Court declared the sanctity of the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law**.**

Modern homes with electronic equipment exchanging information with 3rd parties

However, our modern information age involves exchanging information with third parties, such as phone companies, internet service providers, cable companies, retailers, and so on. Therefore it would seem that clinging to the ancient notion of privacy would mean the practical extinction of privacy in today's world. In contrast to the notion of privacy as secrecy, privacy can be understood as an expectation in a certain degree of accessibility of information. Biometric technologies are changing society and the European Commission's Report of February 2007 into the impact of such technologies, concluded that the burgeoning information society brings with it the need for us to be able to securely identify ourselves quickly and remotely and therefore we need the inevitable implementation of biometric technologies to increase national security, and as a tool to help prevent fraud.

Conclusion

The UK is behind other countries where 'intercepting communications' is concerned. In the US, millions of customers regularly pay for goods and services just be scanning their fingers and punching in a Personal Identification Number ('PIN') instead of using credit or debit card. In Japan, millions of people use contactless palm-scanners to withdraw cash from a bank cash-point. Many laptop computers now have built-in finger scanners. There are now biometric front door locks, garage doors and safes, proving that this is not a 'big brother' technology but that we are in the information age. And there are fingerprint scanners that detect fake fingers. [30]In the UK today, if recordings are secret, they are still inadmissible in civil cases, as per *Chairman and Governors of Amwell School v Dogherty*,

[30] In *U.S. West, Inc. v. Federal Communications Commission* a telecommunications carrier challenged the privacy regulations of the Federal Communications Commission ('FCC'), which restricted the use and disclosure of customers' personal information unless the customers gave their consent. The court stated that: *'A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest, for it is not based on an identified harm.Our names, addresses, types of cars we own, and so on are not intimate facts about our existence, certainly not equivalent to our deeply held secrets or carefully guarded diary entries. In cyberspace, most of our relationships are more like business transactions than intimate interpersonal relationships.'*

Employment Appeal Tribunal. It was decided that unauthorised recordings made by a claimant, of the private deliberations of her employer's disciplinary hearing panel, should not be admitted as evidence in support of her unfair dismissal claim at an employment tribunal on the grounds of public policy. Mr Recorder Luba, QC, said that there was an important public interest, in parties before disciplinary proceedings complying with the ground rules on which the proceedings were based and that no ground rule could be more essential to ensuring a full and frank exchange of views than the understanding that their deliberations would be conducted in private. However, the above case is a far cry from *R v Khan*, a serious criminal case of drug trafficking. The criminal offence of 'possession with intent to supply'/ is determined in the Misuse of Drugs Act 1971, section 5(3) and carries life imprisonment and/or fine in relation to class A drugs. The two situations are incomparable. The UK Regulation of Investigatory Powers Act 2005 contains far reaching powers on telecommunications interception and a decryption order relationship between less privacy and more security. The UK Terrorism Act enables the police to carry out surveillance to prevent terrorism. But surveillance under the UK Terrorism Act is a minor thing compared to the US's Patriot Act 2001. These are some of the surveillance that the Patriot Act allows nationwide search warrant for electronic evidence (ie wire, oral or electronic communications or stored in a remote computer service as described by the Federal wiretap law). In the U.S., nationwide authorisations are obtainable; delayed notice of a search warrant is allowed; and government agencies share information. The U.S. Patriot Act provides for immunity defences for Internet Service Providers when ISPs comply with surveillance and disclosure orders, enabling the government to intercept communications of 'computer trespassers'. In the U.S.voicemails may be seized via search warrants and intercepted information can be shared between agencies. By the US Foreign Intelligence Surveillance Act, there can be multi-point wiretaps.

The introduction of interception powers has created an investigation shift against privacy towards law enforcement. With the exception of investigating telegraphy, which was interceptable from the start and consequently had little expectation of privacy, all telecommunications technologies have known a period of non-interceptability. The balance between criminal investigation and privacy in UK formal law has shifted towards investigation mainly in 2000 by introducing the power of oral interception and the relaxation of several powers to investigate telecommunications. The justification for new investigation powers contain detailed arguments with regard to organised crime.

ISSN 1758-8405

9 771758 840033 03