UK INTERCEPTION OF COMMUNICATIONS (ADMISSIBILITY OF EVIDENCE) BILL 2006

CRIMINAL LAW

2007

ANNOTATIONS AND INTRODUCTORY CHAPTER TO THE BILL WRITTEN BY SALLY RAMAGE IN ANTICIPATION OF THE BILL GAINING ROYAL ASSENT

[BILL ABANDONED ON 16 MARCH 2007]

qwertyuiopasdfghjklzxcvbnmqwertyui
opasdfghjklzxcvbnmqwertyuiopasdfgh
jklzxcvbnmqwertyuiopasdfghjklzxcvb
nmqwertyuiopasdfghjklzxcvbnmqwer
tyuiopasdfghjklzxcvbnmqwertyuiopas
dfghjklzxcvbnmqwertyuiopasdfghjklzx
cvbnmqwertyuiopasdfghjklzxcvbnmq
wertyuiopasdfghjklzxcvbnmqwertyuio
pasdfghjklzxcvbnmqwertyuiopasdfghj
klzxcvbnmqwertyuiopasdfghjklzxcvbn
mqwertyuiopasdfghjklzxcvbnmqwerty
uiopasdfghjklzxcvbnmqwertyuiopasdf
ghjklzxcvbnmqwertyuiopasdfghjklzxc
vbnmqwertyuiopasdfghjklzxcvbnmrty
uiopasdfghjklzxcvbnmqwertyuiopasdf
ghjklzxcvbnmqwertyuiopasdfghjklzxc
vbnmqwertyuiopasdfghjklzxcvbnmqw
ertyuiopasdfghjklzxcvbnmqwertyuiop
asdfghjklzxcvbnmqwertyuiopasdfghjkl

UK INTERCEPTION OF COMMUNICATIONS (AS EVIDENCE) BILL 2007

Introductory Chapter

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 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. The expenditure, administration and policies relating to interceptions for national security purposes are monitored by a statutory parliamentary committee. Members of the public can lodge complaints with the Investigatory Powers Tribunal, which has power to cancel warrants and award compensation. In recent years, legislative amendments have been introduced to enhance the implementation of the interception law and combat terrorism.

Communications interception law in other countries is analysed to throw light on what will occur in the UK if the Interception of Communications Bill 2006 is passed in 2007.

The powers to investigate post, telegraphy, telephony, telecommunications, oral communications and traffic data shows that the balance between criminal investigation and privacy will shift towards law enforcement. As such, privacy may 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. Before 1985[1], there was no overall statutory framework governing the practice which was regulated in part by provisions in various ordinances, and thus its legal basis was obscure. The power was vested in the Secretary of State to authorize by warrant the interception of postal and telegraphic communications, implying that the process was subject to executive control instead of statutory regulation. It was not until 1985 did the government indicate in a White Paper its intention to introduce legislation on interception of communications. The need for legislation was prompted by the European

Following the issuance of the 1985 White Paper, the Interception of Communications Act 1985 (IOCA) was enacted. IOCA placed interception of communications sent by post or through a public telecommunications system on a statutory basis for the first time. It created an offence of unlawful interception of communications, enshrined in law the

[1] 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.

framework for the operation of a warrant system, and set out safeguards, monitoring, and complaint mechanisms.

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-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 regulatory 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.

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 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 statutes are all issued by Judges. Under Title III and FISA, court order applications must be authorized 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 "911" incident, 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.

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[2]. This tension is worse since the recent demand for a society that is totally free from risks. The result is a raft of legislative measures in many countries that target terrorism, some of which are

[2] In the US, the importance of wiretap law to enforcing privacy rights is the case of *Olmstead v. United States[1928]* [1]. The Supreme Court in this case, permitted a police wiretap without a search warrant of telephone calls from a home. Since the 1960's , US wiretaps by both federal and state officials are subject to constitutional scrutiny [5] where there is a reasonable expectation of privacy. According to the most recent Wiretap Report of the Administrative Office of the United States Courts, at least sixty-seven percent of wiretap applications approved in 2001 were authorized by state judges (1,005 of 1,491)[6]. Even more remarkably, while applications approved by federal judges in 2001 increased only one percent from the number authorized in 2000,approvals by state judges rose forty-one percent. The 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.

the US Patriot Act,[3] the Canadian Anti-Terrorism Act, the German Terrorismusbeka¨mpfungsgesetz,[4] 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.

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. relationship between less privacy and more security.

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

[3] The USA PATRIOT Act contains "sunset" provisions so that some of the new surveillance powers were scheduled to expire at the end of 2005.

[4] Not forgetting the German breach of privacy case *Klass v Federal Republic of Germany [1978] 2 EHRR 214* in respect of the German state's use of surveillance devices such as telephone tapping. 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 UK[[1984] 7 EHRR 14*, where the Court found that the domestic law on telephone tapping did not satisfy article 8(2) 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.

enforcement and have bad long-term effects on society as well as the short-term good effect of increased security.

In Australia, interception of communications is principally regulated by a statute known as the Telecommunications (Interception) Act 1979. National security warrants, the application of which must be made by the Director-General of Security, are issued by the Attorney-General. The reasons for issuing such warrants are not necessarily related to particular offences. The application for law enforcement warrants must be made by eligible authorities, and such warrants are issued by Judges or nominated members of a tribunal for the investigation of specified offences. The maximum effective period for national security warrants is twice as long as that for law enforcement warrants. Lawfully intercepted information is admissible as evidence in exempt proceedings or defined circumstances or for permitted purposes. The Ombudsman is empowered to inspect the records of law enforcement warrants. The Attorney-General is required to table annual reports in the Australian Parliament giving details of telecommunications interceptions for law enforcement purposes. Law enforcement and security agencies are accountable to two statutory parliamentary committees.

There have been several significant legislative amendments enacted by the Australian Parliament, most of which are part of the Australian government's measures against terrorism.

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.

Cyber terrorism- A reason for the Interception of Communication as evidence Act2007

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

[5] With online banking fraud increasing by 90% to £23.2 million in 2005, an investigation by the House of Lords into how banks can safeguard our cash has revealed some startling findings regarding online banking. The House of Lords Science and Technology Committee, who are currently investigating personal Internet security, recently heard evidence from representatives of APACS, the UK payments Association, and the credit card company Visa. APACS, written evidence suggested that the number of phishing incidents rose by 8,000% between January 2005 and September 2006. Phishing is the act of sending out an e-mail to a user claiming to be from their bank or other organisation as an attempt to dupe people into supplying them with private information – such as bank details and pin numbers – and then electronically stealing money from their accounts.

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[6]. 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. Recently 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

---

[6] A recent US cyber-terrorist attacked his employers system and the former UBS PaineWebber employee was sentenced to eight years in prison on 11th December 2006 for planting a computer "logic bomb" on company networks and betting its stock would go down. Duronio left his job as a systems administrator in February 2002 after expressing dissatisfaction about his salary and bonuses, then planted malicious computer code known as a "logic bomb" in about 1,000 of PaineWebber's approximately 1,500 networked computers in branch offices. On 4 March, 2002, the "bomb" detonated and began deleting files. Source Reuters 14.12.06.

US," where he says 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.

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 causes 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 cyber attack 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 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 center 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 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".7

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 the rest of us.

---

7 The Wilson Doctrine

On 17 November 1966, Mr Harold Wilson the then Prime Minister, made a statement in the House of Commons that there would be no tapping of the telephones of Members of Parliament but if there was any development of a kind which a change in the general policy, he would, at such moment as seemed compatible with the security of the country, on his own initiative, make a statement in the House of Commons.

51. Some MPs may 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 but it is not, for the following reasons

i. For there to be interception, there must be a Warrant in place, signed by the Secretary of State authorising the interception.

ii. The grounds for doing so are very limited by Section 5(3) of the Act. They are essentially National Security (including terrorism) and the prevention or detection of serious crime.

iii. There is oversight by the Commissioner to prevent wrongful use, and I have made it clear that the Commissioner would personally ensure that there was no improper interception of the communications of any public figure.

Since the Interception of Communications Commissioner only deals with intercepted data or communications traffic data at the level of authorisations, warrants and certificates, how can he possibly "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 ?

People who contact members of Parliament, either their own constituency MPs, or chairmen of committees etc., to complain about the Government, or to reveal some scandal as a "whistleblower", or simply to lobby MPs or Peers to try to influence them to vote in a particular way, should not be inhibited from doing so, by the fear that the Government or its agencies are monitoring their conversations or correspondence with members of Parliament.

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, apart from the 3 intelligence agencies, 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" under legacy legislation, independent of the Regulation of Investigatory Powers Act 2000.

There 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.

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 is preparing a law that would allow 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 seeks such disablement to prevent unauthorised calls made by prison inmates. These mobile phones are often smuggled into prisons despite heavy prison security. Some German Information Technology industry Bitkom group strongly oppose the Bundestag's plans, according to news service Heise Online. Bitkom argues that the plans are technically impraticable. To prevent calls in a soccer stadium or in a prison, the jammer would need a lot of electrical power. Such jamming would result in the block phone conversations in nearby neighbourhoods and cause network instability and quality, Bitkom says.

On a grander scale, the US has created electronic-warfare squads capable of disabling enemy satellite transmissions... The US has established mobile teams equipped with electronic gear capable of disrupting attempts to interfere with its satellite resources[8], Air

[8] [8]The Washington Times reports. (http://www.washtimes.com/national/20050921-102706-1524r.htm)

Force Space Command is tasked with both protecting US satellites from attack Washington Times carried a report that China has tested electronic signal disablement against satellites.. The US Space Command has a responsibility to accessing military threats and is capable of permanently interrupting other countries' capabilities as directed by US policy.

The Australian Communications and Media Authority rejected requests from its government to disable mobile phones in the country's maximum-security prisons. because to do so would interfere with communication devices outside Australia's prisons.

In February 2006, it was reported that eavesdroppers tapped the mobile phones of Greek Prime Minister Costas Karamanlis, cabinet ministers and security officials for a year around the time of the Athens Olympics. The mobile phones of approximately 100 people, including journalists and Greek Arabs, and some of the country's political and security elite, were monitored after such disabling software was illegally installed on the systems of Vodafone- Greece, the country's second largest mobile operator. Spyware enabled phone conversations from Vodafone subscribers to be diverted to 14 pay-as-you-go mobile phones and relayed to a recording system.[9] An official government statement promises of a full judicial investigation. There is speculation that foreign intelligence agencies orchestrated the spying[10]. The Greek government reportedly first learned of this illegal interception in March 2005, through from Vodafone Greece because complaints

---

the Observer newspaper, February 20, 2006.[9]
http://observer.guardian.co.uk/world/story/0, 1702505, 00.html
[10] http://www.athimerini.com/4dcgi/_w_articles_politics_100006_04/02/2006_66009

from unnamed customers over problems with their mobile were traced back to the interception software.'[11].

Interception of communications is necessary to stop frauds and to assist in the conviction of such criminals. Examples of such frauds are as follows:-

US investigators have requested the extradition of four Nigerians accused of running 419 frauds in the Netherlands after the arrest of a gang in Amsterdam and the nearby town of Zaandam earlier this week. It is the first time the US has asked for the extradition of individuals accused of running '419; frauds. DUTCH police arrested 12 people and confiscated €25,000 in cash, computers and forged travel documents. They posted over 100,000 emails to victims in several countries, in particular the US, and gained approximately $2m. The Netherlands remains an important centre for fraudulent lottery and '419; schemes. The emails are sent from other countries. A very prolific group operates out of Italy using Tin-it, Telecom Italia Media's Internet Service Provider. and most of the phone numbers in these e- mails leading to the lottery frauds known as names such as Luckystar, Postcode Loterij and EU Lottery, are Dutch prepaid mobile telephone numbers. Dutch police are investigating another 23 Nigerian gangs after the arrest of 12 suspects in a joint US/Dutch investigation.

[11] Tsalikidis was found hanged in his Athens flat on March 9, only two days after Vodafone Greece had identified and removed the eavesdropping software from its systems, The Times reports (http://www.timesonline.co.uk/article/0, 2089-2025457, 00.html).

Firms suspected of using the malware include Mayer Motors (an importer of Volvo and Honda cars) against Champion Motors (an Audi and Volkswagen dealership), satellite television company Some have been successfully prosecuted in Nigeria..

The convictions are the first by Nigeria's Economic and Financial Crimes Commission (EFCC), established two years ago to combat the country's burgeoning trade in email frauds. [12].

In Hungary, the opposition party admitted that an intern had 'hacked' into the servers of the governing party. The intrusion was traced back to an IP address belonging to Fidesz. Hungarian police have launched an investigation.

United Kingdom communications interception to stop fraud

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.

Many UK businesses are exposed to mobile security risks, according to a new study. Eighty percent of two thousand IT professionals surveyed by market analyst firm Quocirca, say ordinary workers constitute the main mobile security threat.

However, one in five companies that use mobile devices such as wireless Pads and smart phones, have no security policies. Even those, which have mobile security policies, admit

[12] http://go.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=10339658&section=news&src=rss/uk/internetNews

that such policies are rarely enforced. This raise questions about leadership within organisations and whether senior staff treat security as a high priority, according to mobile Telco Orange, which sponsored the online study. The survey found that business managers were content to leave staff responsible for the data security of mobile devices.

An example of interception, which is a criminal offence, resulted in the conviction of criminals Michael and Ruth Haephrati found guilty of industrial espionage in Israel, having been extradited from the UK. The couple were masterminds behind a Spyware-linked industrial espionage program. They had developed and sold customised Spyware or Trojan Horse packages designed to evade detection by security tools. They sold these to three private investigation companies in Israel - Modi'in Ezrahi, Zvi Krochmal, and Philosof-Balali.[13] This Spyware code was installed on victims' Personal Computers by private detectives using a diskette or via email, as part of a spying fraud that ran for up to two years. The Malware sent stolen documents to an FTP site, allowing unscrupulous firms to swipe confidential documents from rivals. Each software installation allegedly netted the Haephratis £2,000. This illegal hacking can only be convicted with evidence gained by police interception and allowable as evidence in court.

Illegal interception of communications in business

5th MARCH 2007 Wal-Mart fires technician for intercepting communications

Walmart has announced that it has terminated a systems technician for intercepting text messages and recording telephone conversations without authorization. The Bentonville, Arkansas, retailing giant Walmart, said the decision follows an internal investigation that started on Jan. 11. The probe found the technician had monitored and recorded

Jerusalem Post.

telephone conversations between Wal-Mart public relations associates and a reporter with The New York Times, which was notified of the situation earlier on Monday. Wal-Mart, a Dow component, added that the technician didn't violate any laws because company policy states its communications systems are subject to monitoring and recording. The company said that it has kept the U.S. Attorney informed throughout the course of its investigation and that it learned on March 1 the U.S. Attorney plans to conduct a probe of the pager intercepts and phone call recordings.
This is one example of how the interception of communications can affect share prices.

Interception of Communications in Cyprus

Various pieces of legislation have been enacted to tackle information technology related offences. More specifically, a law was enacted in 2004 for the purpose of ratifying the European Council's Cyber crime Convention of 2001. The types of offences dealt with concern illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud.

Furthermore, the Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996 (prohibits the unauthorized interception of any private communication, subject to certain exceptions.

The Law Regulating Electronic Communications and Postal services of 2004

(the Electronic Communications Law) prohibits any person, other than users communicating between themselves from time to time, to listen into, tap, store, intercept and/or undertake any other form of surveillance of communications without the consent of the users concerned, except where this is provided for by Law and where there is an authorisation by the Court.

In addition, specific laws such as the Law for the Processing of Personal Data (the Data Protection Law)) penalise spam, unauthorised interference with a record of personal data, receiving knowledge of data, extracting, altering, harming, destroying, processing, transmitting, notifying, making data accessible to unauthorized persons and allowing such persons to receive knowledge of the data, or exploiting the data in any way.

With regards to investigations, this law confers the power to the Commissioner for the Protection of Personal Data to assign officers of his Office the duty to carry out administrative researches and checks of any data record. For this purpose, she has the right to access personal data and to collect any kind of information, without being restricted by any form of confidentiality obligation, except that of legal privilege. However, the Commissioner does not have access to the identity details of her colleagues who are mentioned in records kept for the purposes of national security or for the investigation of particularly serious crimes. Finally, the Commissioner is afforded the power to examine in person records kept for purposes of national security.

www.police.gov.cy

The department of Economic Crime of the Criminal Investigation Office of the Police is in charge of computer crime investigations. It is composed of teams of select detectives that bear the responsibility of the investigations of particularly serious cases on a national basis. In addition, it undertakes the investigation of serious cases, in which the investigations are extended in more than one districts or even abroad. In addition, the department cooperates closely with the Divisional Crime Investigation Departments (Crime Prevention Squads and other departments of the police, for the prevention and investigation of crime.

Furthermore, the Prosecution Office is the direct legal advisor of police detectives and investigators. It is the office they will address for instant advice on issues concerning criminal law, criminal procedure and evidence. It is the contact point between the police and the Law Office of the Republic (Attorney General)). Almost all serious criminal case files are forwarded at the Prosecution Office where experienced criminal lawyers scrutinize them. Many are forwarded to the Law Office with comments and proposals or for consultancy. The rest are returned to the Divisional Police Headquarters with instructions for further investigation, prosecution or final classification. Members of the Prosecution Office undertake the drafting of proposed legislation related to the Police and participate in committees where such bills are discussed. Finally, the Criminalistic situated at the Police Headquarters, is

the main provider of forensic science support to the criminal justice system of the Cyprus Republic.

The courts exercising criminal jurisdiction most likely to deal with computer crime is the District Court of criminal jurisdiction and the Supreme Court of Justice) in its appellate jurisdiction. Criminal proceedings are commenced by a charge preferred at the competent District Court. Every District Judge has jurisdiction to try all offences committed within the district in which the court is established and all offences committed within the Sovereign Base Areas by a Cypriot against a Cypriot.

The Criminal Investigation Office should be alerted in cases of major computer crime incidents, although police experience and willingness to deal with these issues is relatively limited. This is especially so for smaller scale and domestic computer crime incidents reported by private citizens and which involve unauthorised access to transmissions, unauthorised access to information, intrusion attempts and computer fingerprinting. The police are unlikely to give any particular degree of priority in investigating such crimes due to the inadequacy of awareness on such specialised issues.

The Commissioner for the Protection of Personal Data, which is the principal regulatory body dealing with offences such as spam and other unauthorized access to personal information, has the responsibility of ensuring the application of the Data Protection legislation. The Commissioner has a number of powers, inter alia reporting violations of the Law to the competent

authorities and the Police in particular, imposing administrative sanctions, assigning to officers of her Office the duty to carry out administrative searches and making administrative checks of any data record, whether of her own accord or following a report. For this purpose, she has the right to access personal data and collects any kind of information, without being restricted by any form of confidentiality obligation, except that of legal privilege. The Commissioner also has the competence to investigate complaints relevant to the application of the law and the protection of the rights of the applicants when these concern the processing of personal data related to them. She also investigates applications seeking to monitor and ascertain the legality of processing and informs the applicants of her actions.

Finally, the Commissioner of Electronic Communications is conferred power to deal with issues concerning interference with communications networks as well as spam.

Other reporting mechanisms

Cyprus legislation, and in particular the Law Ratifying the Cybercrime Convention of 2001 establishes certain criminal offences in accordance with Chapter II of the Cybercrime Convention in relation to confidentiality, integrity and availability of computer data and systems. In particular, it sanctions:

Computer-Related Forgery:

Section 9 of the Law makes it an offence for a person to, intentionally and without right, input, alter, delete or suppress computer data, resulting in inauthentic data with the intent that such data be considered or acted upon for legal purposes as if they were authentic. This is regardless of the fact that the data were directly readable and intelligible. Such an offence is punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties.

Illicit content:

Offences related to Child Pornography - Section 11 of the Law Ratifying the Cybercrime Convention makes it an offence for a person to intentionally and without right:

(i) Produce child pornography for the purpose of its distribution through a computer system;
(ii) Offer or make available child pornography through a computer system;
(iii) Distribute or transmit (emit) child pornography through a computer system;
(iv) Promote child pornography through a computer system for oneself or for another;
(v) Possess child pornography in a computer system or on a computer-data

storage medium.

Such an offence is punishable with imprisonment for up to ten years or with a fine of up to CYP 25,000 (approx. EUR 43,000) or with both such penalties. The term ‘child pornography’ includes pornographic material that visually depicts a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct as well as realistic images representing a minor engaged in sexually explicit conduct. Sexually explicit conduct is interpreted as to include intercourse between minors or between a minor and a person of age of the same or different sex, sodomy, masturbation, sadistic or masochistic behaviour within the framework of a sexual act.

Attempts, Aiding and Abetting - Section 13 of the Law Ratifying the Cybercrime Convention provides that a person who intentionally and without right aids or abets the commission of any of the offences relevant to illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, offences related to infringements of copyright and related rights, commits an offence punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties.

Racist and Xenophobic Content -

The Law Ratifying the Additional Protocol to the Cybercrime Convention Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature

Committed through Computer Systems establishes the following criminal offences punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties:

(a) Dissemination of Racist and Xenophobic Material through Computer Systems: intentionally and without right distributing or otherwise making available to the public racist and xenophobic material promoting or inciting racial discrimination, hatred or violence, through a computer system.
(b) Racist and Xenophobic Motivated Threats: intentionally and without right threatening a person through a computer system acting on the basis of racism or xenophobia.
(c) Racist and Xenophobic Motivated Insult: intentionally and without right publicly insulting, through a computer system, a person that is, as a result of the insult, found subject to hatred, contempt or ridicule.
(d) Denial, Gross Minimisation, Approval or Justification of Genocide or Crimes Against Humanity: through a computer system, intentionally and without right denying, grossly minimising, approving or justifying acts constituting genocide or crimes against humanity, acting on the basis of racism and xenophobia.
(e) Aiding and Abetting: intentionally and without aiding or abetting the commission of any of the aforementioned offences.

- Specific Obligations Regarding Commercial Communications and

Spamming:

Part II of the Electronic Commerce Law, Sections 9 to 11, prescribes the manner into which commercial communications may be sent by information society service providers for the promotion of goods, services or the image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a profession. Where promotional offers are being sent, such as discounts, premiums and gifts, they must be clearly identifiable as such, and the conditions which are to be met for someone to be able to benefit from the said offers must be easily accessible and the terms must be presented clearly and unambiguously. Promotional competitions or games must also be clearly identifiable as such. The conditions for participation must be easily accessible and the terms must be presented clearly and unambiguously.

Failure to comply with the above provisions may lead to the imposition of a penalty up to CYP 5,000 (approx. EUR 8,700) which may be doubled in the event of second or further conviction

More particularly, with regards to unsolicited commercial communication (spamming), Section 10 of the Law provides that a commercial communication by a service provider established within the territory of the Republic, by electronic mail, with a recipient who has not requested it, must be identifiable clearly and unambiguously as such, as soon as it is received by the recipient. In the event of a violation of these provisions, a person will be liable to a penalty

up to CYP 5,000 (approx. EUR 8,700) which may be doubled in the event of second or further conviction.

Service providers undertaking unsolicited commercial communications by electronic mail must also consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

According to Section 11 of the Law, the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding the independence, dignity and honour of the profession and professional secrecy and fairness towards clients and colleagues.

This Section also confers power to the Minister of Industry, Commerce and Tourism to encourage professional unions and bodies to establish codes of conduct at national and community level in order to determine the types of information that can be given within the framework of commercial communication.

As for reporting mechanisms relevant to spam, Section 4 of the Electronic Commerce Law appoints the Minister of Commerce, Industry and Tourism as the Competent Authority responsible for ensuring the effective application of the Electronic Commerce Law. For this purpose, the Minister is under the

obligation to have available the necessary means of control and investigation and in particular the necessary technical equipment and competent staff for achieving the effective application of the Electronic Commerce Law.

The Minister is also granted the power and function to determine the contact points from which recipients and service providers may refer to by electronic means in order to:

(a) Obtain general information on the applicable legislation on matters relevant to electronic commerce and, in particular, in relation to their contractual rights and obligations as well as on the existing complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;
(b) Obtain the details of authorities, organisations, associations and or other providers in the Republic to which they may refer for further information or practical assistance.

The Electronic Commerce Law imposes a duty on the Minister to investigate violations of the provisions of the Law, either when a complaint is submitted to him or on its own initiative. When carrying out an investigation, the Minister must follow the procedure prescribed by the Law for the purpose of finding whether the provisions of the Law have been violated. Following an investigation, if the Minister considers that there has been a violation and if he deems this to be expedient, he has the power to make an application to the

competent Court for the issuing of an injunction, including an interim order, against any person who, in his judgement, is involved or is responsible for a violation of the Law.

When the Minister exercises the said powers, he must take into consideration all of the interests involved, including the public interest, as well as the promotion of contracts regulated by independent organizations, professional associations and unions and other bodies active in the field of Information Society services.

The Electronic Commerce Law also confers power to the Court before which any application is pending to issue a restraining order, including an interim order ordering:

(a) The immediate seizure and/or non repetition of the violation;
(b) The taking up of such corrective measures according to the Court's judgment, within a prescribed time limit, for the purpose of terminating the illegal situation that has been created by the violation under consideration;
(c) The publication in whole or in part of the relevant decision of the Court or the publication of a restorative notification for the purpose of eliminating any continuing effects of the violation under consideration; and/or
(d) Any other act or measure that it may deem necessary or reasonable under the circumstances of the particular case.

Presentation of Documents

The Evidence Law and the principles established by it apply to any criminal procedure introduced against any person for the punishment thereof for any criminal offence committed in violation of any law or administrative act establishing criminal offences.

According to Section 34 of the Cyprus Law, the competent Court has a discretionary power to admit statements contained in an original document or a copy of an original document, if the statement is admissible as evidence. A 'document' is defined as any object on which any information or representation of any kind is registered or imprinted. A 'copy,' in relation to a document, is defined as anything on which the said information or representation has been copied by use of any medium, either directly or indirectly.

This general definition of the term 'document' has been introduced in 2004 replacing a previous definition which used to take technological developments into account. The previous provision stated that a document included a disc, music tape, electronic disc registering visual representations of writing or any other medium registering visual representations capable of being reproduced either by using another device or without using such device.

Although the new definition does not expressly provide that a document produced electronically is capable of being accepted as evidence, it may be inferred that due to the wide definition of the term, it may include information

or representations reproduced directly or indirectly by electronic mediums. As a result, it may also be inferred that the competent courts are accorded wide discretionary powers with respect to the admissibility of any type of documents, including electronically produced ones.

Presentation of Apparatus, Machines, Equipment – Real Evidence

According to the evidence rules and jurisprudence applicable in Cyprus, an object that is the subject matter of the case or that is relevant to the case before the Court can be presented as evidence to the Court. However, if it is practically impossible to bring it to Court or its visual appearance is not sufficient to lead the Court to conclusions, further evidence may be allowed by persons who came in contact with it, concerning the working condition of the apparatus, its relation to the defendant and the manner in which it was used by the defendant. An expert witness can give such evidence.

Evidence of Tapes, Recordings, Videos, etc

Such material may be admissible evidence and may present a tone of voice or visual characteristic. The registration made by the tape must be precise, strong (not faint) and of good quality and there must be no change or interference. The same is true for video cameras (e.g. attached on buildings). There is no need for the persons who were responsible for the registration to give evidence themselves.

Hearsay Computer Evidence

Evidence from a computer may be admissible as hearsay evidence if evidence is given that the computer was functioning properly and its content has not been altered. Therefore, evidence registered by mechanical means without human interference may be admissible if there is evidence that the machine was functioning properly. Similar provisions apply for discs, tape recorder tapes, sound tapes, or other means such as films, negatives, video tapes and electronic discs for the imprinting of visual representations, where sounds or other elements which are not visual representations are imprinted in a way that they can be reproduced by same with or without the use of other apparatus.

Criminal Procedure

The applicable legislation regarding criminal procedure is the Criminal Procedure Code. This Code basically introduces the English Criminal Procedure Rules with minor modifications.

Arrest of a Person on Reasonable Suspicion of Having Committed an Offence

The Criminal Procedure Code confers the power to the competent Judge, when he is satisfied by written affidavit that there is a reasonable suspicion that a person has committed an offence or when the arrest or the detention is deemed reasonably necessary for preventing the commission of an offence or the escape of the person after the commission thereof, to issue a warrant of arrest

authorising the arrest of the said person.

Search of Premises without a Warrant

Section 25 of the Law confers power on police officers to search without a warrant a person or premises, under certain conditions specified in the said warrant. Concerning premises, a police officer can, inter alia conduct a search without a warrant if he had reason to believe that an offence will or is being committed or has recently been committed. The type of offence must be one punishable with imprisonment exceeding two years. Furthermore, a police officer may enter and search any premises without a warrant by virtue of any legislation in force allowing for this. For example, the Customs And Excise Duties permits such entry and search without a warrant.

Search of Premises with a Warrant (Anton Pillar Order)

A warrant for the search of premises may be issued if the Judge is satisfied that there are reasonable grounds to believe that an item will be found therein intended to be used for the purpose of committing an offence. Here, the purpose is preventive. If the Judge is satisfied as to the necessity of issuing a warrant, he may issue such a warrant and authorize the person named therein to search the specified place and to seize and carry the evidence before the Court. The warrant may also authorise the apprehension of the occupier of the premises who is in possession of the specified object.

Commencement of Criminal Proceedings

Criminal proceedings are commenced by a charge preferred before the competent District Court. The charge is divided in two parts, the statement of the offence and the particulars of the offence. It must be signed by or on behalf of the person preferring same. Such person may be a private citizen, who is aggrieved by an act or omission constituting an offence under the relevant Law. The State may also institute a public prosecution. This right to bring a public prosecution is vested in the Attorney General of the Republic.

- Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996, Law No. 92(I)/1996 - Law Regulating Electronic Communications and Postal services of 2004, Law No. 112(I)/2004 -Law for the Processing of Personal Data (Protection of the Person) Law of 2001, Law No. 138(I)/2001 as amended by Law No. 37(I)/2003 - The Evidence Law,

- Criminal Procedure Code, Cap. 155 as amended by Law No. 93/1972,

,

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 [1967]* 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. three basic categories of investigative techniques. The first category 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. Since *Katz*, the courts have applied the "reasonable expectation of privacy standard" to bugging and wiretap to determine whether a Fourth Amendment "search" has occurred. In this Article, we will use the term "wiretaps" to refer generically to wiretaps and bugging.

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 Supreme Court has held that the Fourth Amendment does not prevent third parties from voluntarily turning over the stored records to law enforcement.[21] In our 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.[22] The Fourth

o

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").[23] 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.[24] The statute also suffered other constitutional infirmities, because it authorized orders of excessive duration; didn't require orders to be promptly executed; 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.[25]

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."[26] 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.[27] Issuance of an order must be based upon a showing of circumstances that justify the use of the

intrusive techniques of interception or eavesdropping.[28] The orders must be for a limited time and subject to a requirement of prompt execution.[29] 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.[30]

These constraints were codified and made more specific in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[31] "Title III," as it is generally called, established substantive and procedural requirements for federal interception orders.[32]

Thereafter was enacted in the US, the Electronic Communications Privacy Act 1986, addressed newer communications technologies such as mobile telephones and electronic mail.[34] The ECPA broadly prohibits all interceptions of the contents of wire, oral, and electronic communications, except where those interceptions comply with the ECPA requirements.[35] 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.[36] 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.[37] 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.[38]

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 appear to be 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.

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.[14] "Private life" covers interference with privacy by surveillance techniques.[15] . "Private life" covers the right to communicate

[14] See *Gaskin v United Kingdom [1990] 12 EHRR 36.*

[1515] See *Malone v United Kingdom [1984] 7 EHRR 14*. In the case *Malone v Metropolitan Police Commissioner (No.2) [1979] Ch 344*, it was held that the plaintiff had no remedy when the police had tapped his telephone because he could not rely on Article 8 of the European Convention (as it had not then been incorporated into English law) and the domestic laws of trespass and confidentiality had not been as a consequence of this ruling Malone went to the European Court of Human Rights .breached on the facts.

private information with others[16]. 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.[17]

In the case *PG and JH v United Kingdom*[18]*, The Times, October 19, 2001*, 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

[16] See *Silver v United Kingdom [1983] 5 EHRR 347*. In this case, a number of prison regulations interfering with the prisoners' right of correspondence were declared to be in violation of Article 8 because they were not sufficiently accessible to be in accordance with the law and were found to be excessive and disproportionate in relation to their legitimate aims of maintaining prison order. The European Court held that the inherent secrecy surrounding telephone tapping carried with it a danger of abuse, requiring clear and accessible legal rules.

[17] See *Halford v United Kingdom [1997] 24 EHRR 523* .In the Halford case, it was held that telephone calls made from business premises were covered by the notion of private life and correspondence under Article 8, and that employees who made calls on internal systems had a reasonable expectation of privacy.

See also *Amman v Switzerland [2000] 30 EHRR 843*. In Amman v Switzerland, it was held that the tapping of the applicant's telephone conversation amounted to a violation of article 8, (which applied to interference executed on business premises)because the national law was not sufficiently clear to clarify the scope and conditions of the authorities' discretionary powers in this area. Th Amman case resulted after a conversation had been tapped, as a result of which the applicant's personal information was placed on a national register.

[18] PG and JH v United Kingdom, the Times, October 19, 2001. The police had placed a covert listening device in the applicant's flat, using such information in subsequent criminal proceedings. 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 with regard to the applicant's telephone, regulated by the Interception of Communications Act 1985, the Court held that as the information had been obtained and used in the context of an investigation and trial concerning a suspected conspiracy to commit robbery, the measures of which were justified under Article 8(2. It was also held that the domestic court was not ion a position to provide effective remedy within Article 13 with respect to any complaint of abuse.

subsequent criminal trials.[19]

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.[20]
The wiretapping case,Malone v United Kingdom case and the bugging devices case Khan v United Kingdom [2001] 31 EHRR 45, resulted in the statute Interception of Communications Act 1985 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.

Right to Privacy in the Workplace in the Information Age

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

[19] See *Khan v United Kingdom [2000] 31 EHRR 45*. It was held that the absence of domestic law regulating the use of bugging devices meant that there had been an unjustified interference with the applicant's private life and correspondence under Article 8. It also held that there had been no violation of Article 6, right to a fair trial when such information from bugging was used to convict the applicant. The conviction was hence based solely on unlawfully obtained evidence. But 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 takes a view of the overall fairness of the trial rather than prescriptively .

[20] See *Peck v United Kingdom [2003] 36 EHRR 41*. The Court held that the disclosure of the footage had resulted in the applicant's actions being observed to an extent far exceeding any exposure to a passer-by or to a security observation and to an extent surpassing that which the applicant could have foreseen. Accordingly, the disclosure by the Council of that footage (even though it was allowed by section 163 Criminal Justice and Public Order Act 1994) had resulted in a serious interference with the applicant's right to respect for private life. With respect to the question of necessity, the Court stressed that such disclosure without the consent of the individual called for the most careful scrutiny by the European Court and could only be justified by an overriding requirement in the public interest.

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

The right to privacy plays a unique role in society. Privacy has also 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.

We can look to other countries when the UK has no precedents

In the US , the Court-made and statutory law have purported to protect a government employees' workplace privacy, however the reality of case law is that the protection afforded to public employees for work-related search and seizure is minimal. The seminal case with regard to the "reasonableness standard," O'Connor v. Ortega, held that the reasonable standard applies to supervisory searches of public employees. Ortega stands

for the proposition that if an employee has a "reasonable expectation of privacy" then one must analyze the reasonableness of the search under the circumstances, i.e., supervision, control and efficiency. Therefore, a public employee has a reasonable expectation of privacy, but it is a qualified one that is subject to the ".operational realities" of the workplace. Although Ortega only focused on public employees the decision implied that private employees were not afforded protection.

Ortega further suggests that E-mail would be considered an employer tool that is used by employees for work-related communications. If this is the case, and the employer's interests outweigh those of the employee, and privacy interests are less in the workplace than in the home, it becomes highly likely that Ortega extends to E-mail with the probable result that E-mail will be precluded from privacy protection.

When analyzing the results of Ortega one needs to ask certain questions concerning future implications of this decision in the workplace such as: (1) What is the impact upon employee efficiency?; (2) Is the employer and employee placed in an adversarial position with regard to the issue of "trust?"; (3) Will there be competitive disadvantages for the employer?; and (4) What about employee dignity?

Subsequent US decisions, such as Schowengerdt v. General Dynamics Corp., have followed Ortega and further weakened, and possibly practically eliminated, an employee's right to privacy in the computerized workplace. Schowengerdt held that the employee had a reasonable expectation to privacy in work areas of exclusive use to the employee, such as the employee's office, unless the employer had previously notified the employee that the employee's office was subject to a work-related search on a regular

basis. The court concluded that despite the employee's reasonable expectation to privacy in his office that a warrant-less search of the office was permissible when it was work-related and reasonable under the circumstances.

US Federal wiretap statute Electronic Communications Privacy Act of 1986 (ECPA) failed to provide sufficient protection for modern computer transmission technologies. The primary purpose of ECPA is to provide protection against unauthorized surveillance of electronic communications. ECPA protection extends to textual information and transmissions of private carriers. ECPA although not specifically providing privacy protection for E-mail systems - court decisions have focused on cellular phone transmissions - does provide protection from unauthorized users who break into the system, steal or manipulate information or damage the system.

The Tort Framework

It may be that the basic legal foundation for private sector employee privacy protection is the common law of torts, specifically privacy protection against the tort of "intrusion". The right to privacy is invaded by the unreasonable intrusion upon the seclusion of another

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 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. And, of course, 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 recently 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.

Companies should distribute the written policy to employees periodically and require them to acknowledge in writing that they've received and understood the policy. Short training sessions—especially for managers charged with enforcing the guidelines—are also a good idea

What should your policy say?

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 is adopted by General Motors, is to require employees and visitors to surrender camera-phones only before entering R&D 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 you choose, 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. In 2007, half of all 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.

However, in the United States, some employers actually distribute camera-phones to their workers. 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. For example, 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 lug heavy products. A real estate agent visiting a property could provide a virtual tour without requiring a client to leave home.

Privacy Issues in a Hi-Tech Workplace

In today's workplace, computers and electronic communications are the norm rather than the exception. Computers, e-mail, electronic databases and on-line research play an

important role in many businesses today. While technological advances have made electronic communication indispensable in today's workplace, the laws regarding privacy issues in the employment area have been ambiguous in the protections they afford to the employer and the employee.

The encryption. process converts data into codes of 1s and 0s and is designed to increase the security of e-mail messages sent over the Internet. This process is designed to increase the security of e-mail messages sent over the Internet. Encryption in the work place, however, is simply not practical, since the technology is not freely exported or widely used.

Most of the US interception case law addresses employers' interception of telephone calls. For example, in Briggs v. American Air Filter Co., 455 F.Supp. 179 (N.D. Ga. 1978) the court found that monitoring business calls of an employee was within the ordinary course of the employer's business and was therefore exempt as a "business exception" under the ECPA Act.

In James v. Newspaper Agency Corp., 591 F. 2d 579, the court similarly found that the business exception applied to a telephone company that monitored telephone conversations between its employees and it customers. The company claimed that the monitoring was necessary to provide better training to its employees.

The court found differently in Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) where the employer's use of a voice logger did not qualify as a telephone or telegraph

instrument. The voice logger monitored telephone calls twenty four hours a day, seven days a week.

The most recent holding regarding electronic privacy in the workplace is Arias v. Mutual Central Alarm Services, Inc., S.D. N.Y., No. 96 Civ. 8447 (LAK and 96 Civ. 8448 (LAK), Sept. 11, 1998. 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.

. In Watkins v. L.M. Berry & Co., 704 F. 2d 577 (11th Cir. 1983) 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.

The case of Bohach v. City of Reno, 932 F.Supp. 1232 (D.Nev. 1996) addresses the question of whether the plaintiffs had a "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

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., 591 F. 2d 579 (10th Cir. 1979), 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., 452 F. Supp. 392 (W.D. Okla. 1978) 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.

In a case somewhat similar to the Simmon's Case, the 5th Circuit in Briggs v. American Air Filter Co., Inc., 630 F. 2d. 414 (5th Cir. 1980), 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., 704 F.2d 577 (11th Cir. 1983), the employer had a policy of monitoring employees sales calls. The employees, however, 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 "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 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, 980 f.2d. 1153 (8th Cir. 1992) 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.

The "business extension" exclusion also 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.

In Deal v. Spears, the 8th Circuit 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, 11 F.3d 271 (4th Cir. 1994), 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., 38 F. 3d 736 (4th Cir. 1994), 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.

Finally, in Pascale v. Carolina Freight Carriers Corp., 898 F.Supp. 276 (D.N.J. 1995), 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 v Interception of Communications

In light of the Interception of Communications (Admissibility of Evidence) Bill 2007, it is a good idea to revisit R *v Khan* and examine the issue of interception of communications as a privacy issue.

To refresh on the facts of *R v Khan*, 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.

This case 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 S.78 PACE 1984.

There was no legal framework regulating the installation and use by the police of covert listening devices. In the light of *R v Sang*[21], the argument that the evidence of the taped conversation was inadmissible could only be sustained if two wholly new principles were

[21] *[1980] AC 402*

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 remained 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 cause of the case coming to the House of Lords was the lack of a statutory system regulating the use of surveillance devices by the police.

The Privacy Issue

Currently, 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"? This question is very important for making legal and policy decisions. Many recognize the importance of privacy for freedom, democracy, social welfare, individual well-being, and other ends. Many also assert it 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.
However, most people fail to understand how privacy should be valued vis-à-vis other interests, such as free speech, effective law enforcement, and other important values.

As the UK has no privacy law, let us look to the US to see how their law treats privacy. In *Olmstead v. United States*[22]. the Court held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespass into the home. But , in 1967, the Court swept away this view in *Katz v. United States*[23], holding that the Fourth

[22], *277 U.S. 438 (1928.*
[23] *389 U.S. 347.* Although the surveillance in this case may have been so narrowly circumscribed that it could constitutionally have been authorized in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance. Pp. 354-359.

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*[24], 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.[1.]

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.*

This 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

[24] *488 U.S. 445 (19890 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.

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 conception in *Union Pacific Railway Co. v. Botsford*[25]. 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.**

As to interception of communication with regard to the home, the US courts have always treated this as a breach of privacy. As early as 1886, in *Boyd v. United States*[26], the US Court strictly protected the sanctity of a man's home The maxim that the home is one's castle appeared as early as 1499. The first recorded case in which this notion was mentioned was *Semayne's Case*[27], In the eighteenth century, William Blackstone declared that the law has "so particular and tender a regard to the immunity of a man's house that it stiles it his castle, and will never suffer it to be violated with impunity." [28]

However, today's Information Age often involves exchanging information with third parties, such as phone companies, internet service providers, cable companies, retailers, and so on. And so, clinging to the ancient notion of privacy as related in the previous

[25] *141 U. S. 250.* The single question presented by this record was whether, in a civil action for an injury to the person, the court, on application of the defendant, and in advance of the trial, may order the plaintiff, without his or her consent, to submit to a surgical examination as to the extent of the injury sued for.
[26] 389 U.S. 347 (1967) Petitioner was convicted under an indictment charging him with transmitting wagering information by telephone across state lines in violation of 18 U.S.C. 1084.
[27] 77 Eng. Rep. 194, 195 (K.B. 1604)
[28] William Blackstone, Commentaries on the Laws of England 223 (1769).

paragraph 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[29]. We read half-baked alarmist articles about interception of communications and breach of privacy yet we in the UK are behind other countries where "intercepting communications" are concerned. It is to be noted that in the US, more than three million customers regularly pay for goods and services just be scanning their fingers and punching in a personal identification number(PIN) instead of using a credit or debit card. In Japan, more than two million people now use contact-less 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.

In U.S. West, Inc. v. Federal Communications Commission[30], a telecommunications carrier challenged the privacy regulations of the Federal Communications Commission

[29] "Privacy & prejudice: whose ID is it anyway?" New Scientist, pg 20, 17 September 2005.

[30] *No. 98-9518, 18TH August 1999.* The dispute in this case involved regulations the FCC promulgated to implement provisions of 47 U.S.C. § 222. Section 222(d) provides three additional exceptions to the privacy requirements.

("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."

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, Employment Appeal Tribunal*[31]. 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.

This case is a far cry from *R v Khan*, a serious criminal case of drug trafficking. Possession with intent to supply is determined in the Misuse of Drugs Act 1971, section

[31] Times, 5th October 2006.

5(3) and carries life imprisonment and/or fine in relation to class A drugs. The two situations are incomparable.

Besides, 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:-

(a) A nationwide search warrant.

(b) For electronic evidence (ie wire, oral or electronic communications or stored in a remote computer service as described by the Federal wiretap law), nationwide authorizations are obtainable.

(c) Delayed notice of a search warrant is allowed.

(d) Government agencies share information.

(e) The 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".

(f) Voicemails may be seized via search warrants.

(g) There can be sharing of intercepted information between agencies, voluntary emergency disclosure of the contents of subscriber communications and records by an ISP and mandatory disclosure pursuant to a court order or warrant.

Also, under the US Foreign Intelligence Surveillance Act, there can be multi-point wiretaps.

My conclusion on the alleged dichotomy between privacy and interception of communications as criminal evidence is that, if the 2007 Bill Interception of Communications is passed, it will put these intercepts on a statutory footing and save much time and money when cases such as *R v Khan* are no longer feasible. ENDS

Conclusion

The introduction of 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 noninterceptability.

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 organized crime Thus, the introduction of investigation powers is mainly argued for from the perspective of the practice of law enforcement: that the police have an urgent need for a power or may derive important information from it. Only when it comes to defining the limits of investigation powers does privacy really come into view. Thus, privacy functions more as a secondary than as a primary factor.

References

B.J.Koops. andA.H. Vedder, (2002), “Criminal investigation and privacy: opinions of citizens”, Computer Law & Security Report, Issue 18: 322–6.

C.J.Sykes, *The End of Privacy*, St Martin’s Press. (New York 1999)

R.Whitaker.*The End of Privacy: How Total Surveillance is Becoming a Reality*, New Press. (New York,1999)

Interception of Communications (Admissibility of Evidence) Bill [HL]

1

A

BILL

TO

Permit the introduction of intercept evidence and evidence of communications data in certain criminal proceedings; and for connected purposes.

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

1 Admissibility of intercept and metering evidence

(1) Notwithstanding section 17 of the Regulation of Investigatory Powers Act 2000 (c. 23) ("RIPA"), evidence of—

(a) the contents of an intercepted communication ("intercept evidence"), and *5*

(b) communications data ("metering evidence"), shall be admissible in criminal proceedings to which this section applies.

(2) This section applies to—

(a) proceedings in respect of serious crime;

(b) proceedings in respect of an offence or offences relating to terrorism. *10*

(3) An application for permission to introduce intercept evidence or metering evidence, or both, may be made by the prosecution for the purpose of conducting a criminal prosecution to which this section applies, and not otherwise.

(4) Unless and until an application has been made by the prosecution in any such *15* proceedings the provisions of section 17 of RIPA (exclusion of matters from legal proceedings) shall continue to apply in connection with those proceedings.

2 Considerations for allowing intercept or metering evidence

In deciding whether to admit intercept or metering evidence the court shall take account of all relevant considerations, including in particular—

(a) any application by the Secretary of State to withhold the evidence or part of the evidence on the ground that its disclosure, or the disclosure

of facts relating to the obtaining of the evidence, would be contrary to the public interest, and

(b) any submission that the evidence was obtained unlawfully.

3 Interpretation

In this Act—

"communications data" has the same meaning as in section 21(4) of RIPA;

"intercepted communication" has the same meaning as in section 4 of RIPA;

"RIPA" means the Regulation of Investigatory Powers Act 2000 (c. 23);

"serious crime" has the same meaning as in section 81(2)(b) of RIPA;

"terrorism" has the same meaning as in the Terrorism Act 2000 (c. 11).

4 Minor and consequential amendments

(1) In section 5(3)(b) of RIPA, for the words "or detecting" substitute ", detecting or prosecuting".

(2) In section 17(1) of RIPA, after the words "Subject to section 18" insert "and the provisions of the Interception of Communications (Admissibility of Evidence) Act 2007".

5 Short title, commencement and extent

(1) This Act may be cited as the Interception of Communications (Admissibility of Evidence) Act 2007.

(2) This Act shall come into force at the end of the period of two months beginning with the day on which the Act is passed.

(3) This Act extends to Northern Ireland.

Interception of Communications (Admissibility of Evidence) Bill [HL]

A

BILL

To permit the introduction of intercept evidence and evidence of communications data in certain criminal proceedings; and for connected purposes.

The Lord Lloyd of Berwick

Ordered to be Printed, 23rd November 2006

INTERCEPTION OF COMMUNICATIONS BILL 2007-09-21 HANSARD NOTES ON ITS DEBATE ON 16 MARCH 2007

Interception of Communications (Admissibility of Evidence) Bill [HL]

1.18 pm

Lord Lloyd of Berwick: My Lords, I beg to move that this Bill be now read a second time.

It is only a week since we last discussed intercept in this House, on the first day in Committee on the Serious Crime Bill. Noble Lords might think that nothing new of importance could have happened between then and now but, if they did, they would be wrong. On Monday this week there was a hearing before the Joint Committee on Human Rights at which two witnesses gave very important evidence for today's debate. One was Sir Swinton Thomas, the retired Interception of Communications Commissioner, and the other Sir Ken Macdonald, the Director of Public Prosecutions.

Sir Swinton made a powerful case for maintaining the status quo, largely on the lines of the report that he published a few weeks ago, which some noble Lords will have seen. To my mind the case made by Sir Ken, the Director of Public Prosecutions, for a change in the law was overwhelming. I shall come back to what he said in a few moments. Sir Ken Macdonald is not the only one to support a change in the law. Last week I gave a long list of others who also support such a change: the noble and learned Lord the Attorney-

General, Lord Goldsmith; Sir David Calvert-Smith, a previous Director of Public Prosecutions; Sir Ian Blair; the noble Lord, Lord Carlile, the independent watchdog in these matters appointed by the Government, and so on. I shall quote a former chief constable of the West Midlands and Inspector of Constabulary, the noble Lord, Lord Dear, whom I am very glad to see in his place. He said that he had for 10 years or more been in favour of admitting this evidence and added:

> "It is interesting to see the tide not just turning but running strongly in favour of this proposal".—[*Official Report*, 7/3/07; col. 305.]

Quite so.

The first question that always arises in these debates is whether admission of intercept evidence would do any good: whether it would increase the number of suspects who can be brought to court and, it is hoped, convicted. Nobody, of course, suggests that it would lead to convictions in every case of serious crime, but it is common ground now that it would lead to more convictions in some cases of serious crime. That has been common ground ever since the Home Office review of February 2005; it is also the Minister's own view. She has told us on many occasions that she is altogether in favour of admission of intercepts if it can be done safely. She described it last week as,

> "a consummation devoutly to be wished".—[*Official Report*, 7/3/07; col. 313.]

Sir Swinton Thomas is of the same view, though he expressed that sentiment in slightly more judicious language as becomes a retired judge. The question comes down simply to this: can we or can we not do it safely? Can we find a way of making evidence admissible without prejudicing what we already have? My answer is: yes we can.

Two arguments are always used the other way, and no doubt we shall hear them again today from the noble Baroness, Lady Ramsay, whom I am very glad to see in her place. The first is that if criminals knew that their telephone conversations could be intercepted, they would cease to use the telephone and we would thereby lose a valuable source of intelligence. I do not doubt for one moment that telephone intercept is a very valuable source of intelligence—that, again, is common ground—but I suggest that there is nothing in the argument that we would lose that ability. We are talking here, after all, of serious organised crime committed by sophisticated criminals operating across national boundaries. Of course they know that their conversations can be intercepted; otherwise, they would not talk in the guarded terms in which they speak so often. They know that in every other country that evidence can be used in court against them; yet, they continue to use the telephone for communicating with each other to hatch their conspiracies because they have no other means of communicating with each other. It is fanciful to suppose that the habits of these criminals would change because the evidence was at long last to be made admissible in the United Kingdom as well as in every other country in the world.

The second argument is that if intercept evidence were allowed in court, criminals would soon discover the methods by which it was obtained. This is what worries the security

service and GCHQ. I assure your Lordships that I understand their concern, but the courts are not quite so naïve in this respect as some may imagine. In common with every other common-law country, we have developed a means of protecting sensitive information that is thought to be at risk in some way. The principle is called public interest immunity; there is nothing new about it. It is well understood in the courts. I do not say that it is used every day but it is used very frequently. The procedure is set out in Part 25 of the Criminal Procedure Rules 2005. If lawyers for the defence demanded to see documents that might disclose methods of intercept, the application would come before the judge who would hear the case and decide whether the documents should be disclosed. It is inconceivable that a judge would order documents to be disclosed, or information to be discovered, that would reveal methods used by GCHQ and other agencies. If the judge went off his head and did so order, the prosecution would at once appeal to the Court of Appeal, which would put the situation right. If the Court of Appeal went off their collective heads, there would always be an appeal to your Lordships' House. There is therefore nothing in the two main arguments against allowing intercept, which have been used so often.

If anybody doubted the utility of intercept evidence, or our ability to use it safely, I hope that your Lordships will look at the position in the United States and Australia, on which the evidence of Sir Ken Macdonald is very revealing and important. In September 2004 he visited his opposite numbers in the United States and Australia. He talked to eight agencies in the United States and 12 in Australia. Everywhere he got the same message: it would make an enormous difference. I should like to read out a great deal of his evidence but I cannot; however, I shall read just two or three sentences:

> "Colleagues in the Department of Justice in the United States have told us that the majority of their major prosecutions now against terrorist figures and organised crime figures are based upon intercept evidence. I think it is well known that for the first time each of the five New York crime godfathers are in prison, each of them as a result of the use of intercept evidence. In Australia, I was told by the head of the New South Wales Crime Commission that prosecutors who did not rely on intercept evidence were not being 'serious' in this area of work".

That evidence given by Sir Ken is amply borne out in the report by Justice, which refers to an observation of Mr Damian Bugg QC, the Australian federal Director of Public Prosecutions, who says:

> "We rarely now have a drug importation prosecution that does not have telephone intercept evidence in it. I can think of any number of prosecutions where we would have real difficulty in prosecuting without it—we just would not get the evidence".

It is evidence of that kind which makes it difficult to understand the statistics which the Minister gave, as reported at col. 310 of *Hansard*.

Sir Kenneth was asked about something that the noble Baroness said last week. It was put to him that the noble Baroness had said that,

> "the evidential use of intercept would not even add significantly to the number of convictions that can be secured".—[*Official Report*, 7/3/07; col. 310.]

When asked whether he agreed with that, he said that he disagreed profoundly. Nowhere in those other jurisdictions has it been suggested that, because of the use of intercept in this way, the methods of those carrying out the interceptions have been revealed. The question then is: if those other countries can do it safely, why cannot we?

Another arguments used by the noble Baroness last week was that, if we use intercept evidence, the prosecution would have to disclose everything, there would be a great mass of material, and that would add greatly to the length and cost of trials. That is not the case. Of course there is an obligation to disclose material that would help the defence or undermine the prosecution, but there is no obligation to disclose material described as neutral. That was the decision of the House of Lords not long ago in R v H, reported in 2004 Appeal Cases. Then there was the argument that we might run into difficulties under the European Convention on Human Rights. There was a reference to the principle of equality of arms. That does not touch on this question. The court of human rights has made it clear that there is no absolute right to disclosure; disclosure is always subject to the overriding interest of national security. That was decided in Rowe and Davis v United Kingdom in 2000.

The noble Baroness said that, in a few years' time, present methods of intercepting conversations would be out of date and obsolete. Instead, we will have voice over internet protocol, or voice over IP. I am sure she is right that that is the way in which it is moving, but I am not sure how it affects the question that the House is debating now. To find out more about that, if I could, I had a conversation only last night with David Craig, who works for a Scottish company called Agilent Technologies. He was in San Francisco, and I was at home. The conversation took place by means of voice over IP. I could not notice any difference between that conversation and any that I have had over the telephone. He told me that voice over IP can be intercepted; it is more difficult to intercept than mobile phones or landlines, but it can be done. The problems are not insuperable. Indeed, about 150 companies worldwide have the capability of doing that. Whether or not that is so, I cannot see that it really affects this question. If there is to be new technology and we are going to be able to get intercept from it, by all means let us use it in court.

Two other arguments were advanced by the noble Baroness. First, that the admission of intercept in court would in some way imperil the close relationship between the intelligence agencies and the law enforcement agencies. I have heard that argument advanced on numerous occasions, but I have never begun to understand it. She said that the intelligence agencies might not be willing to co-operate with the police once intercept was used evidentially, or at least that co-operation might be endangered. They are both government agencies; surely if the national interest requires the use of intercept to secure convictions, the intelligence agencies can be persuaded to co-operate with the police.

Of course there will be resource implications, but if we are to be serious about convicting criminals, against whom there may be no other evidence, we must not let resource implications stand in the way. In fact, again Sir Ken Macdonald explained in his evidence that the use of intercept would be very cost-effective, because it leads to shorter not longer trials and to more guilty pleas. He gave some very interesting figures to bear out that view. I will leave the last word to Sir Kenneth:

> "Everybody without exception told us that this material is of enormous use. It is cheap, it is effective; it drives up the number of guilty pleas and it leads to successful prosecutions. We are convinced, and have been for a number of years, that this material will be of enormous benefit to us in bringing prosecutions against serious criminals, including terrorists".

I commend the Bill to the House.

Moved, That the Bill be now read a second time.—(*Lord Lloyd of Berwick*.)

1.36 pm

Lord Boyd of Duncansby: My Lords, the Justice report, to which the noble and learned Lord made reference, tells us that one of the early examples of the use of intercept evidence was the trial of Mary, Queen of Scots, in 1586. She was convicted in the October of treason, following the interception of letters that revealed her knowledge of Babington's plot. She was subsequently beheaded at Fotheringay Castle in 1588. If it is thought that the citation of that triumph of English justice would persuade me of the merits of this legislation, I am afraid that is mistaken.

This issue has been debated many times in your Lordships House over a number of years. While I am new to the public debate, I am not new to the argument, which I followed for some time while I was in government. While others who have had experience and responsibility in this area have spoken publicly, so far I have kept my own counsel. I want today to set out why I think that the position adopted by the Government is correct and why I believe that it would be premature at this stage to lift the ban on the use of intercept evidence in court.

When I was first called on to consider this matter in detail in 2001 or 2002, my instinctive reaction was that anything that assisted in the prosecution of serious crime and of terrorist offences was greatly to be welcomed. That remains my instinctive reaction. If we can devise a system that would meet the legitimate concerns of those in the intelligence community who have expressed their views and meet the considerable burden on the criminal justice system, I would welcome that. However, at present we are right to be sceptical, and we are right to accept the Government's position.

In the first place, doubts were expressed about the number of occasions when intercept evidence would be useful in bringing prosecutions. I was aware of the review being undertaken in government, which was reported in January 2005. It was referred to in the

Minister's speech last week and today by the noble and learned Lord, Lord Lloyd of Berwick. It concluded that there would be a modest increase in the conviction rate of some lower-and medium-level criminals, but not terrorists. When I left office, I was not aware of any change in that situation, although, to be fair, I had not checked that in the month before I left office. However, any change would clearly be a material factor.
