Law Enforcement Techniques

Kimi Turnbull

First Edition, 2012

ISBN 978-81-323-2413-3

Published by:
Library Press
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter- 1

Surveillance

A 'nest' of surveillance cameras at the Gillette Stadium in Foxborough, Massachusetts

Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people and often in a surreptitious manner. It most usually refers to observation of individuals or groups by government organizations, but disease surveillance, for example, is monitoring the progress of a disease in a community.

The word *surveillance* is the French word for "watching over".

The word *surveillance* may be applied to observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls). It may also refer to simple, relatively no- or low-technology methods such as human intelligence agents and postal interception.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program and ADVISE, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of their subjects.

However, many civil rights and privacy groups such as the Electronic Frontier Foundation and ACLU have expressed concern that by allowing continual increases in government surveillance of citizens that we will end up in a mass surveillance society, with extremely limited, or non-existent political and/or personal freedoms. Fears such as this have led to numerous lawsuits such as Hepting v. AT&T.

Types of surveillance

Computer surveillance

Official seal of the Information Awareness Office -- a U.S. agency which developed technologies for mass surveillance

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies.

There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups. Billions of dollars per year are spent, by agencies such as the Information Awareness Office, NSA, and the FBI, to develop, purchase, implement, and operate systems such as Carnivore, NarusInsight, and ECHELON to intercept and analyze all of this data, and extract only the information which is useful to law enforcement and intelligence agencies.

Computers are also a surveillance target because of the personal data stored on them. If someone is able to install software (either physically or remotely), such as the FBI's "Magic Lantern" and CIPAV, on a computer system, they can easily gain unauthorized access to this data.

Another form of computer surveillance, known as TEMPEST, involves reading electromagnetic emanations from computing devices in order to extract data from them at distances of hundreds of meters.

The NSA also runs a database known as "Pinwale", which stores and indexes large numbers of emails of both American citizens and foreigners.

Telephones and mobile telephones

The official and unofficial tapping of telephone lines is widespread. In the United States for instance, the Communications Assistance For Law Enforcement Act (CALEA) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies. Two major telecommunications companies in the U.S. -- AT&T and Verizon—have contracts with the FBI, requiring them to keep their phone call records easily searchable and accessible for Federal agencies, in return for $1.8 million dollars per year. Between 2003 and 2005, the FBI sent out more than 140,000 "National Security Letters" ordering phone companies to hand over information about their customers' calling and Internet histories. About half of these letters requested information on U.S. citizens.

Human agents are not required to monitor most calls. Speech-to-text software creates machine-readable text from intercepted audio, which is then processed by automated call-analysis programs, such as those developed by agencies such as the Information

Awareness Office, or companies such as Verint, and Narus, which search for certain words or phrases, to decide whether to dedicate a human agent to the call.

Law enforcement and intelligence services in the U.K. and the United States possess technology to remotely activate the microphones in cell phones, by accessing the phone's diagnostic/maintenance features, in order to listen to conversations that take place nearby the person who holds the phone.

Mobile phones are also commonly used to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily (whether it is being used or not), using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. A controversy has emerged in the United States over the legality of such techniques, and particularly whether a court warrant is required. Records for *one* carrier alone (Sprint), showed that in a given year federal law enforcement agencies requested customer location data 8 million times.

Surveillance cameras

Citizens under surveillance in Cairns, Queensland

Surveillance cameras such as these are installed by the millions in many countries, and are nowadays monitored by automated computer programs instead of humans.

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device, IP network, and/or watched by a security guard/law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage. Now with cheaper production techniques, it is simple and inexpensive enough to be used in home security systems, and for everyday surveillance. Analysis of footage is made easier by automated software that organizes digital video footage into a searchable database, and by automated video analysis software (such as VIRAT and HumanID). The amount of footage is also drastically reduced by motion sensors which only record when motion is detected.

The use of surveillance cameras by governments and businesses has dramatically increased over the last 10 years. In the U.K., for example, there are about 4.2 million surveillance cameras—1 camera for every 14 people.

In the United States, the Department of Homeland Security gives billions of dollars per year in Homeland Security grants for local, state, and federal agencies to install modern

video surveillance equipment. For example, the city of Chicago, IL recently used a $5.1 million Homeland Security grant to install an additional 250 surveillance cameras, and connect them to a centralized monitoring center, along with its preexisting network of over 2000 cameras in a program known as Operation Virtual Shield. Chicago Mayor Richard Daley has announced that Chicago will have a surveillance camera on every street corner by the year 2016.

As part of China's Golden Shield Project, several U.S. corporations such as IBM, General Electric, and Honeywell have been working closely with the Chinese government to install millions of surveillance cameras throughout China, along with advanced video analytics and facial recognition software, which will identify and track individuals everywhere they go. They will be connected to a centralized database and monitoring station, which will, upon completion of the project, contain a picture of the face of every person in China: over 1.3 billion people. Lin Jiang Huai, the head of China's "Information Security Technology" office (which is in charge of the project), credits the surveillance systems in the United States and the U.K. as the inspiration for what he is doing with the Golden Shield project.

Payload surveillance camera manufactured by Controp and distributed to the U.S. Government by ADI Technologies.

The Defense Advanced Research Projects Agency (DARPA) is funding a research project called Combat Zones That See that will link up cameras across a city to a centralized monitoring station, identify and track individuals and vehicles as they move through the city, and report "suspicious" activity (such as waving arms, looking side-to-side, standing in a group, etc.).

At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida, used Identix's facial recognition software, FaceIt, to scan the crowd for potential criminals and terrorists in attendance at the event. (it found 19 people with pending arrest warrants)

Governments often initially claim that cameras are meant to be used for traffic control, but many of them end up using them for general surveillance. For example, Washington, D.C. had 5000 "traffic" cameras installed under this premise, and then after they were all in place, networked them all together and then granted access to the Metropolitan Police Department, so that they could perform "day-to-day monitoring".

The development of centralized networks of CCTV cameras watching public areas—linked to computer databases of people's pictures and identity (biometric data), able to track peoples' movements throughout the city, and identify who they have been with—has been argued by some to present a risk to civil liberties.

Social Network Analysis

One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database, and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.

Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are currently investing heavily in research involving social network analysis. The intelligence community believes that the biggest threat to U.S. power comes from decentralized, leaderless, geographically dispersed groups of terrorists, subversives, extremists, and dissidents. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network.

Jason Ethier of Northeastern University, in his study of modern social network analysis, said the following of the Scalable Social Network Analysis Program developed by the Information Awareness Office:

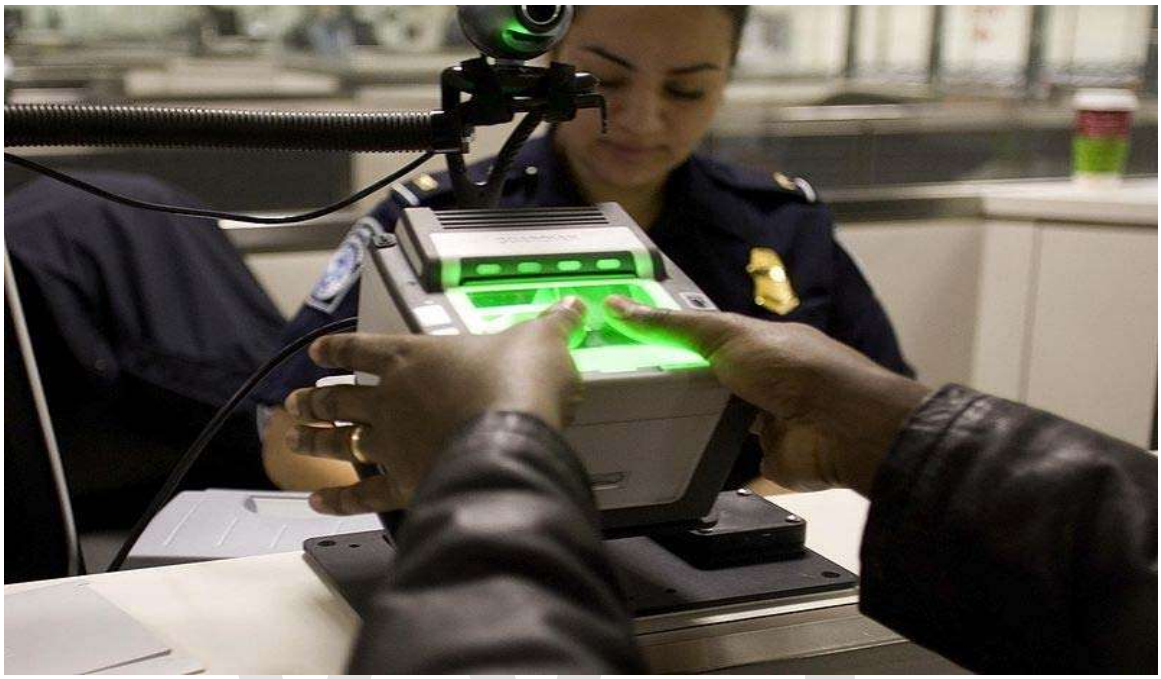
The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people ... In order to be successful SSNA will require information on the social interactions of the majority of people around the globe. Since the Defense Department cannot easily distinguish between peaceful citizens and terrorists, it will be necessary for them to gather data on innocent civilians as well as on potential terrorists.
—Jason Ethier

AT&T developed a programming language called "Hancock" which is able to sift through enormous databases of phone call and Internet traffic records, such as the NSA call database and extract "communities of interest" -- groups of people who call each other regularly, or groups that regularly visit certain sites on the Internet. AT&T originally built the system to develop "marketing leads", but the FBI has regularly requested such information from phone companies such as AT&T without a warrant, and after using the data stores all information received in its own databases, regardless of whether or not the information was ever useful in an investigation.

Some people believe that the use of social networking sites is a form of "participatory surveillance", where users of these sites are essentially performing surveillance on

themselves, putting detailed personal information on public websites where it can be viewed by corporations and governments. About 20% of employers have reported using social networking sites to collect personal data on prospective or current employees.

Biometric surveillance



Fingerprints being scanned as part of the US-VISIT program

Biometric surveillance refers to technologies that measure and analyze human physical and/or behavioral characteristics for authentication, identification, or screening purposes. Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioral characteristics include gait (a person's manner of walking) or voice.

Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video. Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems. The Information Processing Technology Office, ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft by their facial features.

Another form of behavioral biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioral traits. This might be used for instance to see if a person is acting "suspicious" (looking around furtively, "tense" or "angry" facial expressions, waving arms, etc.).

A more recent development is DNA fingerprinting, which looks at some of the major markers in the body's DNA to produce a match. The FBI is currently spending $1 billion to build a new biometric database, which will store DNA, facial recognition data, iris/retina (eye) data, fingerprints, palm prints, and other biometric data of people living in the United States. The computers running the database will be contained in an underground facility is about the size of a football field.

The Los Angeles Police Department is currently installing automated facial recognition and license plate recognition devices in its squad cars, and providing handheld face scanners, which officers will use to identify people while on patrol.

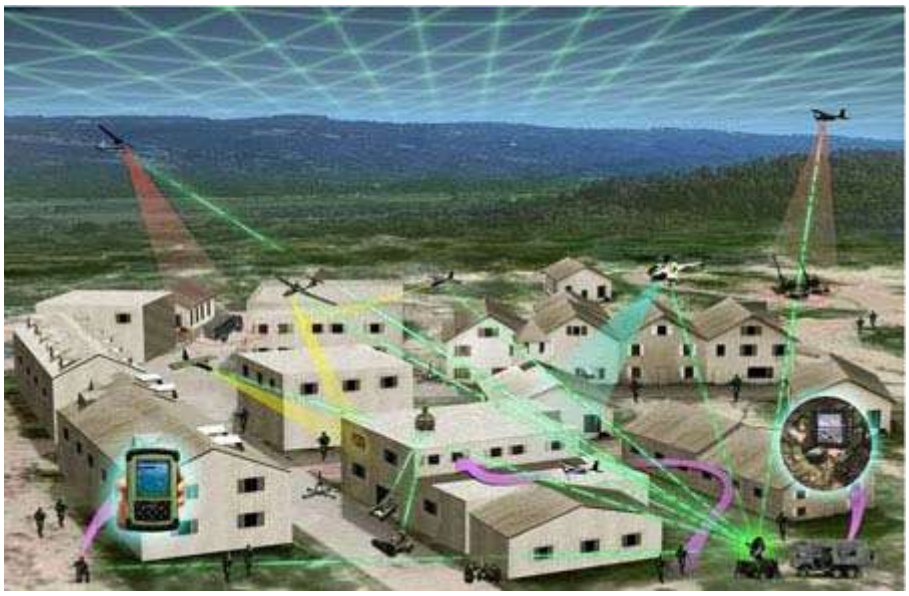
Facial thermographs are currently in development, which allow machines to identify certain emotions in people such as fear or stress, by measuring the temperature generated by blood flow to different parts of their face. Law enforcement officers believe that this has potential for them to identify when a suspect is nervous, which might indicate that they are hiding something, lying, or worried about something.

Aerial surveillance

Micro Air Vehicle with attached surveillance camera

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle—such as a unmanned aerial vehicle, helicopter, or spy plane.

Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper, a U.S. drone plane currently used for domestic operations by the Department of Homeland Security, carries cameras that are capable of identifying an object the size of a milk carton from altitudes of 60,000 feet, and has forward-looking infrared devices that can detect the heat from a human body at distances of up to 60 kilometers.



HART program concept drawing from official IPTO (DARPA) official website

The United States Department of Homeland Security is in the process of testing UAVs to patrol the skies over the United States for the purposes of critical infrastructure protection, border patrol, "transit monitoring" and general surveillance of the U.S. population. Miami-Dade police department ran tests with a vertical take-off and landing UAV from Honeywell, which is planned to be used in SWAT operations. Houston's police department has been testing fixed-wing UAVs for use in "traffic control".

The U.K., as well, is currently working on plans to build up a fleet of surveillance UAVs ranging from micro-aerial vehicles to full-size drones, to be used by police forces throughout the U.K.

In addition to their surveillance capabilities, MAVs are capable of carrying tasers for "crowd control", or weapons for killing enemy combatants.

Programs such as the Heterogenous Aerial Reconnaissance Team program developed by DARPA have automated much of the aerial surveillance process. They have developed

systems consisting of large teams drone planes that pilot themselves, automatically decide who is "suspicious" and how to go about monitoring them, coordinate their activities with other drones nearby, and notify human operators if something suspicious is occurring. This greatly increases the amount of area that can be continuously monitored, while reducing the number of human operators required. Thus a swarm of automated, self-directing drones can automatically patrol a city and track suspicious individuals, reporting their activities back to a centralized monitoring station.

Data mining & profiling

Data mining is the application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data.. Data profiling in this context is the process of assembling information about a particular individual or group in order to generate a profile — that is, a picture of their patterns and behavior. Data profiling can be an extremely powerful tool for psychological and social network analysis. A skilled analyst can discover facts about a person that they might not even be consciously aware of themselves.

Economic (such as credit card purchases) and social (such as telephone calls and emails) transactions in modern society create large amounts of stored data and records. In the past this data would be documented in paper records and would leave a "paper trail", or simply not be documented at all. Correlation of paper-based records was a laborious process—it required human intelligence operators to manually dig through documents, which was time-consuming and incomplete, at best.

But today many of these records are electronic, resulting in an "electronic trail". Every use of a bank machine, payment by credit card, use of a phone card, call from home, checked out library book, rented video, or otherwise complete recorded transaction generates an electronic record. Public records—such as birth, court, tax and other records—are increasily being digitized and made available online. In addition, due to laws like CALEA, web traffic and online purchases are also available for profiling. Electronic record-keeping makes data easily collectable, storable, and accessible—so that high-volume, efficient aggregation and analysis is possible at significantly lower costs.

Information relating to many of these individual transactions is often easily available because it is not generally not guarded in isolation, since the information, such as the title of a movie a person has rented, might not seem sensitive. However, when many such transactions are aggregated they can be used to assemble a detailed profile revealing the actions, habits, beliefs, locations frequented, social connections, and preferences of the individual. This profile is then used, by programs such as ADVISE and TALON, to determine whether the person is a military, criminal, or political threat.

In addition to its own aggregation and profiling tools, the government is able to access information from third parties — for example, banks, credit companies or employers, etc. — by requesting access informally, by compelling access through the use of subpoenas or other procedures, or by purchasing data from commercial data aggregators

or data brokers. The United States has currently spent $370 million on its 43 planned fusion centers, which are national network of surveillance centers that are located in over 30 states. The centers will collect and analyze vast amounts of data on U.S. citizens. It will get this data by consolidating personal information from sources such as state driver's licensing agencies, hospital records, criminal records, school records, credit bureaus, banks, etc. -- and placing this information in a centralized database that can be accessed from all of the centers, as well as other federal law enforcement and intelligence agencies.

Under *United States v. Miller* (1976), data held by third parties is generally not subject to Fourth Amendment warrant requirements.

Corporate Surveillance

Corporate surveillance is the monitoring of a person or group's behavior by a corporation. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. It can be used as a form of business intelligence, which enables the corporation to better tailor their products and/or services to be desirable by their customers. Or the data can be sold to other corporations, so that they can use it for the aforementioned purpose. Or it can be used for direct marketing purposes, such as the targeted advertisements on Google and Yahoo, where ads are targeted to the user of the search engine by analyzing their search history and emails (if they use free webmail services), which is kept in a database.

For instance, Google, the world's most popular search engine, stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months. Google also scans the content of emails of users of its Gmail webmail service, in order to create targeted advertising based on what people are talking about in their personal email correspondences. Google is, by far, the largest Internet advertising agency—millions of sites place Google's advertising banners and links on their websites, in order to earn money from visitors who click on the ads. Each page containing Google ads adds, reads, and modifies "cookies" on each visitor's computer. These cookies track the user across all of these sites, and gather information about their web surfing habits, keeping track of which sites they visit, and what they do when they are on these sites. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use for building a profile of the user to deliver better-targeted advertising.

The United States government often gains access to these databases, either by producing a warrant for it, or by simply asking. The Department of Homeland Security has openly stated that it uses data collected from consumer credit and direct marketing agencies—such as Google—for augmenting the profiles of individuals that it is monitoring. The FBI, Department of Homeland Security, and other intelligence agencies have formed an "information-sharing" partnership with over 34,000 corporations as part of their Infragard program.

The U.S. Federal government has gathered information from grocery store "discount card" programs, which track customers' shopping patterns and store them in databases, in order to look for "terrorists" by analyzing shoppers' buying patterns.

Human operatives

Organizations that have enemies who wish to gather information about the groups members or activities face the issue of infiltration.

In addition to operatives infiltrating an organization, the surveilling party may put pressure on certain members of the target organization to act as informants (i.e. disclose the information they hold on the organization and its members).

Fielding operatives is very expensive, and for governments with wide-reaching electronic surveillance tools at their disposal the information recovered from operatives can often be obtained from less problematic forms of surveillance such as those mentioned above. Nevertheless, human infiltrators are still common today. For instance, in 2007 documents surfaced showing that the FBI was planning to field a total of 15,000 undercover agents and informants in response to a anti-terrorism directive sent out by George W. Bush in 2004 that ordered intelligence and law enforcement agencies to increase their HUMINT capabilities.

Satellite Imagery

On May 25, 2007 the U.S. Director of National Intelligence Michael McConnell authorized the National Applications Office (NAO) of the Department of Homeland Security to allow local, state, and domestic Federal agencies to access imagery from military intelligence satellites and aircraft sensors which can now be used to observe the activities of U.S. citizens. The satellites and aircraft sensors will be able to penetrate cloud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and will provide real-time video at much higher resolutions than the still-images produced by programs such as Google Earth.

Identification & Credentials

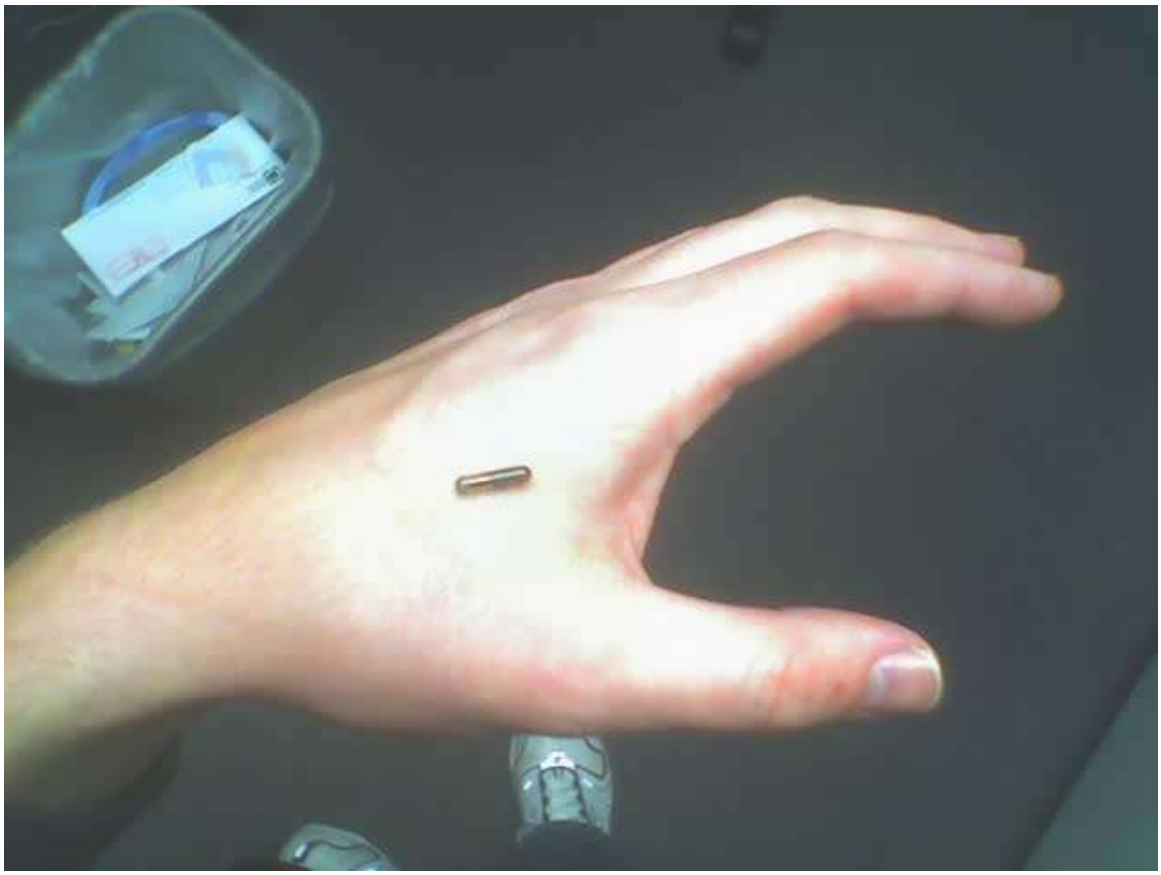
A card containing an identification number

One of the simplest forms of identification is the carrying of credentials. Some nations have an identity card system to aid identification, whilst many, such as Britain, are

considering it but face public opposition. Other documents, such as driver's licenses, library cards, bankers or credit cards are also used to verify identity.

If the form of the identity card is "machine-readable," usually using an encoded magnetic stripe or identification number (such as a Social Security number) that corroborates the subject's identifying data. In this case it may create a document trail when it is checked and scanned, which can be used in profiling, as mentioned above.

RFID & Geolocation Devices



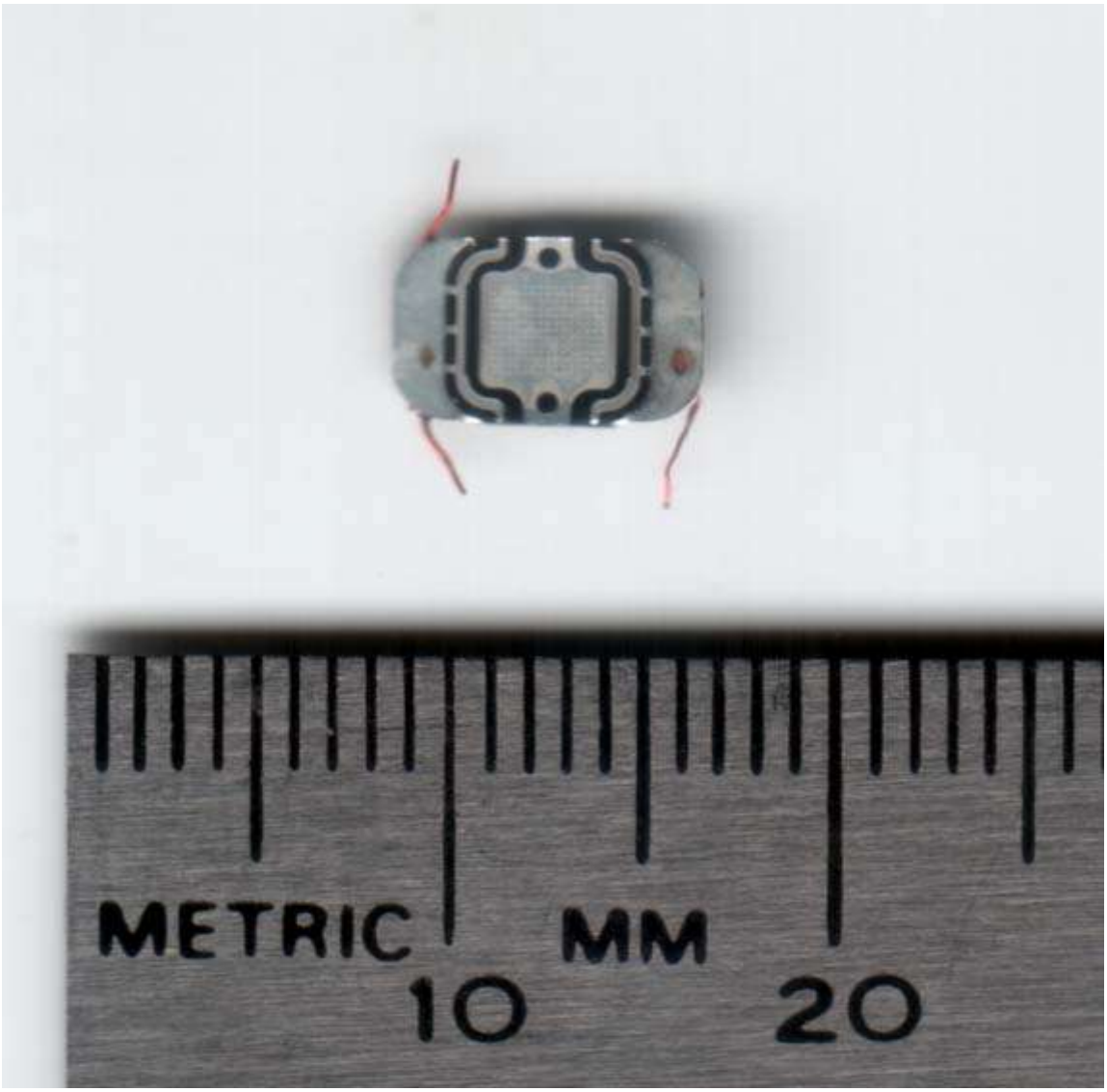
Hand with planned insertion point for Verichip device

RFID tagging

Radio Frequency Identification (RFID) tagging is the use of very small electronic devices (called 'RFID tags') which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are extremely cheap, costing a few cents a piece, so they can be inserted into many types of everyday products without significantly increasing the price, and can be used to track and identify these objects for a variety of purposes.

Many companies are already "tagging" their workers, who are monitored while on the job. Workers in U.K. went on general strike in protest of having themselves tagged. They

felt that it was dehumanizing to have all of their movements tracked with RFID chips. Some critics have expressed fears that people will soon be tracked and scanned everywhere they go.



RFID chip pulled from new credit card

Verichip is an RFID device produced by a company called Applied Digital Solutions (ADS). Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc.'s database, the "Global VeriChip Subscriber Registry". Thousands of people have already had them inserted. In Mexico, for example, 160 workers at the Attorney General's office were required to have the chip injected for identity verification and access control purposes.

It may be that soon every object that is purchased, and perhaps ID cards, will have RFID devices in them, which would broadcast information about people as they walk past scanners (what type of phone they have, what type of shoes they have on, which books they are carrying, what credit cards or membership cards they have, etc.). This information could be used for identification, tracking, or targeted marketing.

Global Positioning Systems (GPS)

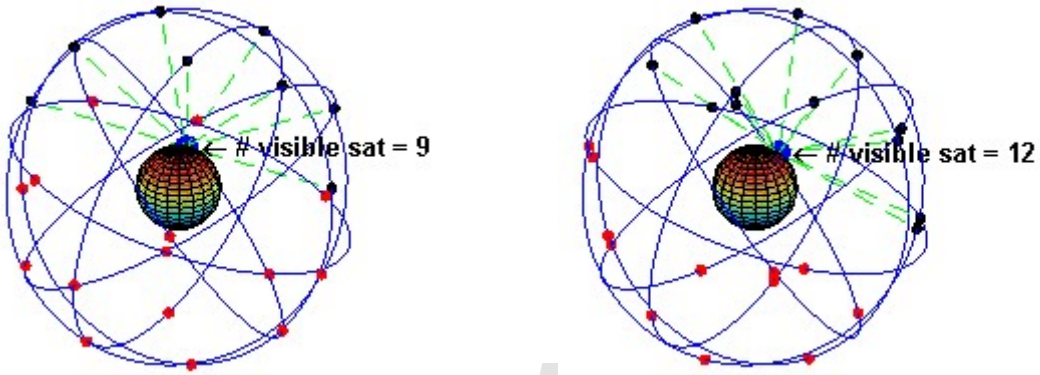


Diagram of GPS satellites currently orbiting Earth

In the U.S., police have planted hidden GPS tracking devices in people's vehicles to monitor their movements, without a warrant. In early 2009 they were arguing in court that they have the right to do this.

Several cities are running pilot projects to require parolees to wear GPS devices to track their movements when they get out of prison.

Mobile phones

Mobile phones are also commonly used to collect geolocation data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily (whether it is being used or not), using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone.

Surveillance devices, or "bugs"

Surveillance devices, or "bugs", are hidden electronic devices which are used to capture, record, and/or transmit data to a receiving party such as a law enforcement agency.

The U.S. has run numerous domestic intelligence, such as COINTELPRO, which have bugged the homes, offices, and vehicles of thousands of U.S. citizens, usually political activists, subversives, and criminals.

Law enforcement and intelligence services in the U.K. and the United States possess technology to remotely activate the microphones in cell phones, by accessing the phone's diagnostic/maintenance features, in order to listen to conversations that take place nearby the person who holds the phone.

Postal services

As more people use faxes and e-mail the significance of surveilling the postal system is decreasing, in favor of Internet and telephone surveillance. But interception of post is still an available option for law enforcement and intelligence agencies, in certain circumstances.

The CIA and FBI have performed twelve separate mail-opening campaigns targeted towards U.S. citizens. In one of these programs, more than 215,000 communications were intercepted, opened, and photographed.

Controversy surrounding surveillance

Graffiti expressing concern about proliferation of video surveillance

Support

Some supporters of surveillance systems believe that these tools protect society from terrorists and criminals. Other supporters simply believe that there is nothing that can be done about it, and that people must become accustomed to having no privacy. As Sun Microsystems CEO Scott McNealy said: "You have zero privacy anyway. Get over it."

Another common argument is: *"If you aren't doing something wrong then you don't have anything to fear."* Some critics state that this claim should be modified to read: *"As long as we do what we're told, we have nothing to fear."*. For instance, a person who is part of a political group which opposes the policies of the national government, might not want the government to know their names and what they have been reading, so that the government cannot easily subvert their organization, arrest them, or kill them. Other critics state that while a person might not have anything to hide right now, the government might later implement policies that they do wish to oppose, and that opposition might then be impossible due to mass surveillance enabling the government to identify and remove political threats. Other critics point to the fact that most people *do* have things to hide. For example, if a person is looking for a new job, they might not want their current employer to know this.

Opposition

Totalitarianism

A traffic camera atop a high pole oversees a road in the Canadian city of Toronto.

Programs such as the Total Information Awareness program, and laws such as the Communications Assistance For Law Enforcement Act have led many groups to fear that society is moving towards a state of mass surveillance with severely limited personal, social, political freedoms, where dissenting individuals or groups will be strategically removed in COINTELPRO-like purges.

Kate Martin, of the Center For National Security Studies said of the use of military spy satellites being used to monitor the activities of U.S. citizens: *"They are laying the bricks one at a time for a police state."*

Psychological/Social Effects

Some critics, such as Michel Foucault, believe that in addition to its obvious function of identifying and capturing individuals who are committing undesirable acts, surveillance also functions to create in everyone a feeling of always being watched, so that they become self-policing. This allows the State to control the populace without having to resort to physical force, which is expensive and otherwise problematic.

Privacy

Numerous civil rights groups and privacy groups oppose surveillance as a violation of people's right to privacy. Such groups include: Electronic Privacy Information Center, Electronic Frontier Foundation, ACLU

There have been several lawsuits such as Hepting v. AT&T and EPIC v. Department of Justice by groups or individuals, opposing certain surveillance activities.

Legislative proceedings such as those that took place during the Church Committee, which investigated domestic intelligence programs such as COINTELPRO, have also weighed the pros and cons of surveillance.

Countersurveillance, inverse surveillance, sousveillance

Countersurveillance is the practice of avoiding surveillance or making surveillance difficult. With recent developments — the Internet, increasing prevalence of electronic security systems, armed UAVs flying at 60,000 feet, and large corporate/government computer databases — counter surveillance has dramatically grown in scope and complexity.

Inverse surveillance is the practice of reversalism on surveillance (e.g., citizens photographing police). Well-known examples are George Holliday's recording of the Rodney King beating and the organization Copwatch, which attempts to surveil police officers to prevent police brutality.

Sousveillance (a term coined by Steve Mann, a professor at the University of Toronto) is inverse surveillance that includes the recording of an activity by a participant in the activity.

Chapter- 2

Interrogation Techniques

Five techniques

The term **five techniques** refers to certain interrogation practices adopted by the Northern Ireland and British governments during Operation Demetrius in the early 1970s. These methods were adopted by the Royal Ulster Constabulary with training and advice regarding their use coming from senior intelligence officials in the United Kingdom Government.

The five techniques were **wall-standing, hooding, subjection to noise, deprivation of sleep, and deprivation of food and drink**. In 1978, the European Court of Human Rights (ECHR) trial "Ireland v. the United Kingdom" ruled that the five techniques "did not occasion suffering of the particular intensity and cruelty implied by the word torture ... [but] amounted to a practice of inhuman and degrading treatment", in breach of the European Convention on Human Rights.

Parker Report

In response to the public and Parliamentary disquiet on 16 November 1971, the Government commissioned a committee of inquiry chaired by Lord Parker, the Lord Chief Justice of England to look into the legal and moral aspects of the use of the five techniques.

The "Parker Report" was published on 2 March 1972, and had found the five techniques to be illegal under domestic law:

10. Domestic Law ...(c) We have received both written and oral representations from many legal bodies and individual lawyers from both England and Northern Ireland. There has been no dissent from the view that the procedures are illegal alike by the law of England and the law of Northern Ireland. ... (d) This being so, no Army Directive and no Minister could lawfully or validly have authorized the use of the procedures. Only Parliament can alter the law. The procedures were and are illegal.

On the same day (2 March 1972), the United Kingdom Prime Minister Edward Heath stated in the House of Commons:

The Government, having reviewed the whole matter with great care and with reference to any future operations, have decided that the techniques ... will not be used in future as an aid to interrogation... The statement that I have made covers all future circumstances.

"As foreshadowed in the Prime Minister's statement, directives expressly prohibiting the use of the techniques, whether singly or in combination, were then issued to the security forces by the Government." These are still in force and the use of such methods by UK security forces would not be condoned by the Government.

European Commission of Human Rights inquiries and findings

The Irish Government on behalf of the men who had been subject to the five methods took a case to the European Commission on Human Rights (Ireland v. United Kingdom, 1976 Y.B. Eur. Conv. on Hum. Rts. 512, 748, 788-94 (Eur. Comm'n of Hum. Rts.)). The Commission stated that it

considered the combined use of the five methods to amount to torture, on the grounds that (1) the intensity of the stress caused by techniques creating sensory deprivation "directly affects the personality physically and mentally"; and (2) "the systematic application of the techniques for the purpose of inducing a person to give information shows a clear resemblance to those methods of systematic torture which have been known over the ages..a modern system of torture falling into the same category as those systems.applied in previous times as a means of obtaining information and confessions.

European Court of Human Rights trial Ireland v. the United Kingdom

The Commission's findings were appealed. In 1978 in the European Court of Human Rights (ECHR) trial "Ireland v. the United Kingdom" (Case No. 5310/71) the facts were not in dispute and the judges court published the following in their judgement:

These methods, sometimes termed "disorientation" or "sensory deprivation" techniques, were not used in any cases other than the fourteen so indicated above. It emerges from the Commission's establishment of the facts that the techniques consisted of:

- (a) wall-standing: forcing the detainees to remain for periods of some hours in a "stress position", described by those who underwent it as being "spreadeagled against the wall, with their fingers put high above the head against the wall, the legs spread apart and the feet back, causing them to stand on their toes with the weight of the body mainly on the fingers";
- (b) hooding: putting a black or navy coloured bag over the detainees' heads and, at least initially, keeping it there all the time except during interrogation;
- (c) subjection to noise: pending their interrogations, holding the detainees in a room where there was a continuous loud and hissing noise;

- (d) deprivation of sleep: pending their interrogations, depriving the detainees of sleep;
- (e) deprivation of food and drink: subjecting the detainees to a reduced diet during their stay at the centre and pending interrogations.

These were referred to by the court as the **five techniques**. The court ruled:

167. ... Although the five techniques, as applied in combination, undoubtedly amounted to inhuman and degrading treatment, although their object was the extraction of confessions, the naming of others and/or information and although they were used systematically, **they did not occasion suffering of the particular intensity and cruelty implied by the word torture** as so understood. ...
168. The Court concludes that recourse to the five techniques **amounted to a practice of inhuman and degrading treatment**, which practice was in breach of *[the European Convention on Human Rights]* Article 3 (art. 3).

On 8 February 1977, in proceedings before the ECHR, and in line with the findings of the Parker report and United Kingdom Government policy, the Attorney-General of the United Kingdom stated that

The Government of the United Kingdom have considered the question of the use of the 'five techniques' with very great care and with particular regard to Article 3 (art. 3) of the Convention. They now give this unqualified undertaking, that the 'five techniques' will not in any circumstances be reintroduced as an aid to interrogation.

Medical torture

Medical torture (also known as a **medical interrogation**) describes the involvement and sometimes active participation of medical professionals in acts of torture, either to judge what victims can endure, to apply treatments which will enhance torture, or as torturers in their own right. Medical torture may involve the use of their expert medical knowledge to facilitate interrogation or corporal punishment, in the conduct of torturous human experimentation or in providing professional medical sanction and approval for the torture of prisoners. The term also covers torturous scientific (or pseudo-scientific) experimentation upon unwilling human subjects.

Medical ethics and international law

It is generally accepted that medical torture fundamentally violates medical ethics, which all medical practitioners are expected to adhere to.

- The Hippocratic Oath makes explicit statements against deliberate harm not in the patient's best interests. These statements are often translated as *"I will prescribe regimens for the good of my patients according to my ability and my judgement"* and *"to never deliberately do harm to anyone, for anyone else's interest."* (Note: these statements are formulations of the ethical principles of beneficence and non-maleficence.)
- In response to the Nazi human experimentation on prisoners, which were declared at the Nuremberg Trials to be "crimes against humanity", the World Medical Association developed the Declaration of Geneva to supplant the dated Hippocratic Oath. The Declaration of Geneva requires medical practitioners to state "[I, the medical practitioner] will maintain the utmost respect for human life from its beginning even under threat and I will not use my medical knowledge contrary to the laws of humanity".
- The Nuremberg Trials also led to the emergence of the Nuremberg code which explicitly outlines the boundaries of acceptable medical experimentation.
- Additionally in response to the Nazi atrocities, the Fourth Geneva Convention of 1949 outright prohibits the torture of prisoners of war and other protected non-combatants.
- The World Medical Association Declaration of Tokyo (1975) makes a number of specific statements against torture, including "The doctor shall not *countenance*, *condone* or *participate in* the practice of torture".
- Also the UN Convention Against Torture, which applies not only to medical staff, prohibits the use of torture under any circumstance. The text explicitely states there is no exception to this treaty under which torture is allowed.
- The UN Principles of Medical Ethiks relevant to the Role of Health Personnel, particularly Physicians, in the Protection of Prisoners and Detainees against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (UN.1982) applies specifically to medical and other health workers but it has no implementation mechanism to ensure enforcement. It is up to state, provincial, and national bodies to enforce the standards in the document.
- The development of command responsibility established criminal liability for all people, including physicians, involved in crimes against humanity.

There remain gaps in regulation relating to medical torture in many countries:

- Government sponsored torture and organized violence, with the complicity and or participation of health personnel, is internationally prohibited yet these violations occur with impunity in a significant amount of cases. An example of this impunity is found in the Abu Ghraib prison torture and prisoner scandal as well as documented by Amnesty International.

- A higher standard of behaviour is expected of health professionals yet the UN Principles of Medical Ethics are not enforceable when governments are complicit in violations. This higher standard is reflected in the principles of beneficence, non-maleficence (above all do no harm), autonomy, justice, dignity and informed

consent and these aren't covered comprehensively by the UN Convention Against Torture.

Asserted instances

- Between 1937 and 1945, Japanese medical personnel who were part of Unit 731 participated in the torture killings of as many as 10,000 Chinese, Russian, American and other prisoners as well as Allied POWs during the second Sino-Japanese War.
- During World War II, Unit 731 of the Japanese Imperial Army tried out various biological weapons on Chinese subjects.
- During World War II, the Nazi regime in Germany conducted human medical experimentation on large numbers of people held in its concentration camps. In particular, Josef Mengele's experiments on prisoners at Auschwitz earned him the nicknames "the Angel of Death" and "Dr. Death".
- Japanese surgeons also performed vivisection and other medical experiments to torture American prisoners of war in several islands of the Pacific.
- Between 1970 and 1971, mentally disorienting interrogation techniques were used against interned prisoners captured in Northern Ireland, including white noise. The Irish government complained to the European Commission for Human Rights, who found Britain guilty of torture; however the higher European Court of Human Rights ruled that the British government's actions were "inhuman and degrading but did not constitute torture".
- In Soviet mental hospitals, used to hold political prisoners, very unpleasant medications were given to these "patients" as a means of punishment. A psychiatric diagnosis was devised to describe people who oppose government policies.
- In 1978, "Pisaot menuh" ("Human Experiments") were performed on seventeen political prisoners held at the infamous prison Tuol Sleng in Phnom Penh under the Khmer Rouge.
- A study called "The Aversion Project" found that gay conscripts in the South African Defense Forces (SADF) during the apartheid era had been forced to submit to "curing" their homosexuality, both by electroshock therapies and by botched sex changes.
- There have been numerous claims that electroconvulsive therapy and prefrontal lobotomies and similar psychiatric treatments have sometimes been performed not in the patient's best interests, but rather as punishment for misbehaviour or to otherwise make the patient easier to manage. A classic example of this is the Lake Alice, New Zealand atrocity which occurred in the early 1970s. Children admitted to the Lake Alice Hospital's open child and adolescent unit were routinely punished with unmodified electroconvulsive treatment. Some governments (e.g. Norway and New Zealand) have since begun paying reparations to patients who suffered such treatments. The World Health Organization has called for a ban on unmodified ECT, and states no form of it should be used on children.

Asserted medical or professional complicity

According to the Center for Constitutional Rights' When Healers Harm campaign, health professionals were complicit in the torture and abuse of detainees during the so-called "war on terror" of U.S. President George W. Bush. Health professionals are those who are trained or licensed in a healing profession, including: medical doctors, psychiatrists, medical examiners, psychologists, and nurses. All of these professions have been implicated in the torture and abuse of prisoners in CIA secret prisons and in military detention centers, such as those in Guantánamo, Afghanistan, and Iraq.

Among other things, health professionals:

- crafted abusive tactics and falsely legitimized their use;
- advised interrogators on methods of abuse that would exploit prisoners' vulnerabilities;
- used medical procedures to harm prisoners;
- gauged pain and monitored interrogations that risked leaving prisoners in need of treatment;
- checked prisoners to certify that they were capable of surviving additional abuse;
- conditioned medical or mental health treatment on cooperation with interrogation;
- shared confidential patient information that was used to harm patients;
- covered up evidence of torture and abuse; and
- turned a blind eye to cruel treatment.

State licensing boards and the professional associations have the responsibility to uphold medical ethics and to hold medical professionals accountable for their participation in abuse. To date, none of these bodies has investigated – nor, in some cases, even acknowledged – abusive conduct by individual members of their professions. In 2009, after years of denial, the American Psychological Association finally recognized that psychologists had engaged in torture. However, the American Psychological Association has yet to acknowledge that psychologists were in fact integral to the Bush Administration's torture policy. Some criticize the APA for failing to respond to allegations of "collusion between APA officials and the national security apparatus in providing ethical cover for psychologists' participation in detainee abuse."

Although the American Medical Association has made clear that physicians should not be involved in interrogations of any kind, it continues to insist that it has "no specific knowledge of doctors being involved in abuse or torture," despite widely known evidence to the contrary, including government documents and Office of Legal Counsel memos, a report by the International Committee of the Red Cross and multiple accounts by survivors.

Today, under President Barack Obama's watch, certain forms of abuse continue.

Some other accounts of medical or professional complicity in torture include:

- The SERE ("Survival, Evasion, Resistance and Escape") program's chief psychologist, Col. Morgan Banks, issued guidance in early 2003 for the "behavioral science consultants" who helped to devise Guantánamo's interrogation strategy although he has emphatically denied that he had advocated the use of SERE counter-resistance techniques to break down detainees. The *New Yorker* notes that in November, 2001 Banks was detailed to Afghanistan, where he spent four months at Bagram Air Base, "supporting combat operations against Al Qaeda and Taliban fighters".
- A 2005 report by Human Rights Watch suggested that torture was routine under the appointed Iraqi government. Human Rights Watch Report
- Dr. J.C. Carothers, British colonial Kenyan psychiatrist, has been implicated in designing interrogation of Mau Mau prisoners.
- Similarly, it has been implied that Interim Iraqi Prime Minister Dr. Ayad Allawi violated his obligation to medical ethics whilst serving as Western European chief of secret police for the Baathist government of Saddam Hussein. However, the same sources allege that Allawi had abandoned his medical education at that point and his medical degree "was conferred upon him by the Baath party."

Third degree

The third degree is a euphemism for the "inflicting of pain, physical or mental, to extract confessions or statements". In 1931 the Wickersham Commission found that use of the third degree was widespread in the United States. No one knows the origin of the term but there are several hypotheses. The use of the third degree was technically made illegal after the Wickersham report. However, the interrogation method known as the Reid technique, which is now widely used by law enforcement in the U.S., is seen by many as simply a psychological version of the third degree in that it's equally capable of extracting a false confession through coercion when abused by police.

Possible origins

- The third degree of Freemasonry and the rigorous procedures to advance to that level.
- The term may have been coined by Richard H. Sylvester, the Chief of Police for Washington, DC. He divided police procedures into the arrest as the first degree, transportation to jail as the second degree, and interrogation as the third degree.
- The term may have been coined by nineteenth century New York City Police detective Thomas F. Byrnes, perhaps as a pun on his name, as in *third degree burns*.

Chapter- 3

Enhanced Interrogation Techniques

Enhanced interrogation techniques or **alternative set of procedures** were terms adopted by the George W. Bush administration in the United States to describe interrogation methods used by US military intelligence and the Central Intelligence Agency (CIA) to extract information from individuals captured in the "War on Terror" soon after the September 11 attacks in 2001.

The Obama administration in 2009 concluded that the techniques amount to torture and prohibited their use.

Central Intelligence Agency

A Congressinal bipartisan report in December 2008 established that:

harsh interrogation techniques used by the CIA and the U.S. military were directly adapted from the training techniques used to prepare special forces personnel to resist interrogation by enemies that torture and abuse prisoners. The techniques included forced nudity, painful stress positions, sleep deprivation, and until 2003, waterboarding, a form of simulated drowning.

Depiction of waterboarding during protest demonstration

According to ABC News, former and current CIA officials have come forward to reveal details of interrogation techniques authorized in the CIA. These include:

1. Attention Grab: The interrogator forcefully grabs the shirt front of the prisoner and shakes them
2. Attention Slap: An open-handed slap to the face aimed at causing pain and triggering fear
3. Belly Slap: A hard open-handed slap to the abdomen. The aim is to cause pain, but not internal injury. Doctors consulted advised against using a punch, which could cause lasting internal damage
4. Long Time Standing: This technique is described as among the most effective. Prisoners are forced to stand, handcuffed and with their feet shackled to an eye bolt in the floor, for more than 40 hours
5. Cold Cell: The prisoner is left to stand naked in a cell kept near 50 degrees Fahrenheit (10 degrees Celsius), while being regularly doused with cold water.
6. Waterboarding: The prisoner is bound to an inclined board, feet raised and head slightly below the feet. Material is wrapped over the prisoner's face and water is poured over them. Unavoidably, the gag reflex kicks in and a terrifying fear of drowning leads to almost instant pleas to bring the treatment to a halt

In December 2007 CIA director Michael Hayden stated that "of about 100 prisoners held to date in the CIA program, the enhanced techniques were used on about 30, and waterboarding used on just three."

According to an item on ABC news in 2007 the CIA removed waterboarding from its list of enhanced interrogation techniques in 2006. ABC stated further that the last use of waterboarding was in 2003.

Department of Defense

The following techniques were being used by the U.S. military:

1. Yelling
2. Loud music, and light control
3. Environmental manipulation
4. Sleep deprivation/adjustment
5. Stress positions
6. 20-hour interrogations
7. Controlled fear (muzzled dogs)

In November 2006, former US army Brigadier General Janis Karpinski, in charge of Abu Ghraib prison until early 2004, told Spain's *El Pais* newspaper she had seen a letter signed by United States Secretary of Defense Donald Rumsfeld that allowed civilian contractors to use techniques such as sleep deprivation during interrogation.'"The methods consisted of making prisoners stand for long periods, sleep deprivation ... playing music at full volume, having to sit in uncomfortably ... Rumsfeld authorised these specific techniques." She said that this was contrary to the Geneva Conventions and quoted from the same: "Prisoners of war who refuse to answer may not be threatened, insulted, or exposed to any unpleasant or disadvantageous treatment of any kind". According to Karpinski, the handwritten signature was above his printed name and in the same handwriting in the margin was written: "Make sure this is accomplished".

On May 1, 2005, *The New York Times* reported on an ongoing high-level military investigation into accusations of detainee abuse at Guantánamo, conducted by Lieutenant General Randall M. Schmidt of the Air Force, and dealing with: "accounts by agents for the Federal Bureau of Investigation who complained after witnessing detainees subjected to several forms of harsh treatment. The FBI agents wrote in memorandums that were never meant to be disclosed publicly that they had seen female interrogators forcibly squeeze male prisoners' genitals, and that they had witnessed other detainees stripped and shackled low to the floor for many hours."

On July 12, 2005, members of a military panel told the committee that they proposed disciplining prison commander Major General Geoffrey Miller over the interrogation of Mohammed al Qahtani, who was forced to wear a bra, dance with another man, and threatened with dogs. The recommendation was overruled by General Bantz J. Craddock, commander of US Southern Command, who referred the matter to the army's inspector general.

In an interview with AP on February 14, 2008 Paul Rester, chief military interrogator at Guantanamo Bay and director of the Joint Intelligence Group, said most of the

information gathered from detainees came from non-coercive questioning and "rapport building," not harsh interrogation methods.

Development of techniques, and training

West coast, Navy SERE Insignia

The CIA interrogation strategies were based on work done by James Elmer Mitchell and Bruce Jessen in the Air Force's Survival Evasion Resistance Escape (SERE) program. The CIA contracted with the two psychologists to develop alternative, harsh interrogation techniques. However, neither of the two psychologists had any experience in conducting interrogations. Air Force Reserve Colonel Steve Kleinman stated that the CIA "chose two clinical psychologists who had no intelligence background whatsoever, who had never conducted an interrogation... to do something that had never been proven in the real world." Associates of Mitchell and Jessen were skeptical of their methods and believed they did not possess any data about the impact of SERE training on the human psyche. The CIA came to learn that Mitchell and Jessen's expertise in waterboarding was probably "misrepresented" and thus, there was no reason to believe it was medically safe or effective. Despite these shortcomings of experience and know-how, the two psychologists boasted of being paid $1000 a day plus expenses, tax-free by the CIA for their work.

The SERE program, which Mitchell and Jessen would reverse engineer, was originally designed to be defensive in nature and was used to train pilots and other soldiers on how to resist harsh interrogation techniques and torture were they to fall into enemy hands. The program subjected trainees to torture techniques such as “waterboarding . . . sleep deprivation, isolation, exposure to extreme temperatures, enclosure in tiny spaces, bombardment with agonizing sounds at extremely damaging decibel levels, and religious and sexual humiliation.” Under CIA supervision, Miller and Jessen adapted SERE into an offensive program designed to train CIA agents on how to use the harsh interrogation

techniques to gather information from terrorist detainees. In fact, all of the tactics listed above would later be reported in the International Committee of the Red Cross Report on Fourteen High Value Detainees in CIA Custody as having been used on Abu Zubaydah.

Stephen Soldz, Steven Reisner and Brad Olson wrote an article describing how the techniques used mimic what was taught in the SERE-program: "the military's Survival, Evasion, Resistance, and Escape program that trains US Special Operations Forces, aviators and others at high risk of capture on the battlefield to evade capture and to resist 'breaking' under torture, particularly through giving false confessions or collaborating with their captors".

The psychologists relied heavily on experiments done by American psychologist Martin Seligman in the 1970s known as “learned helplessness.” In these experiments caged dogs were exposed to severe electric shocks in a random way in order to completely break their will to resist. Mitchell and Jessen applied this idea to Abu Zubaydah during his interrogation. Many of the interrogation techniques used in the SERE program, including waterboarding, cold cell, long-time standing, and sleep deprivation were previously considered illegal under U.S. and international law and treaties at the time of Abu Zubaydah’s capture. In fact, the United States had prosecuted Japanese military officials after World War II and American soldiers after the Vietnam War for waterboarding and as recently as 1983. Since 1930, the United States had defined sleep deprivation as an illegal form of torture. Many other techniques developed by the CIA constitute inhuman and degrading treatment and torture under the United Nations Convention against Torture and Article 3 of the European Convention on Human Rights.

According to Human Rights First:

Internal FBI memos and press reports have pointed to SERE training as the basis for some of the harshest techniques authorised for use on detainees by the Pentagon in 2002 and 2003.

And Salon stated:

A March 22, 2005, sworn statement by the former chief of the Interrogation Control Element at Guantánamo said instructors from SERE also taught their methods to interrogators of the prisoners in Cuba.

While Jane Mayer reported for *The New Yorker*:

According to the sere affiliate and two other sources familiar with the program, after September 11th several psychologists versed in SERE techniques began advising interrogators at Guantánamo Bay and elsewhere. Some of these psychologists essentially “tried to reverse-engineer” the SERE program, as the affiliate put it. “They took good knowledge and used it in a bad way,” another of the sources said. Interrogators and BSCT members at Guantánamo adopted coercive techniques similar to those employed in the SERE program.

and continues to report:

many of the interrogation methods used in SERE training seem to have been applied at Guantánamo.."

A bipartisan report in released 2008 stated that:

a February 2002 memorandum signed by President George W. Bush, stating that the Third Geneva Convention guaranteeing humane treatment to prisoners of war did not apply to al-Qaeda or Taliban detainees, and a December 2002 memo signed by former Defense Secretary Donald Rumsfeld, approving the use of "aggressive techniques" against detainees held at Guantanamo Bay, as key factors that lead to the extensive abuses.

Approval of techniques by U.S. officials

In early 2002, immediately following Abu Zubaydah's capture, top US Government officials including Dick Cheney, Colin Powell, George Tenet, Condoleezza Rice, Donald Rumsfeld, and John Ashcroft discussed at length whether or not the CIA could legally use harsh techniques against Abu Zubaydah. Condoleezza Rice specifically mentioned the SERE program during the meeting stating "I recall being told that U.S. military personnel were subjected to training to certain physical and psychological interrogation techniques…"

ABC News reported on April 9, 2008 that "the most senior Bush administration officials discussed and approved specific details of how high-value al Qaeda suspects would be interrogated by the Central Intelligence Agency." The article states that those involved included:

Vice President Cheney, former National Security Advisor Condoleezza Rice, Defense Secretary Donald Rumsfeld and Secretary of State Colin Powell, as well as CIA Director George Tenet and Attorney General John Ashcroft.

In addition, in 2002 and 2003, several Democratic congressional leaders were briefed on the proposed "enhanced interrogation techniques." These congressional leaders included Nancy Pelosi, the future Speaker of the House, and Representative Jane Harman. Congressional officials have stated that the attitude in the briefings was "quiet acquiescence, if not downright support." Senator Bob Graham, who CIA records claim was present at the briefings, has stated that he was not briefed on waterboarding in 2002 and that CIA attendance records clash with his personal journal. Harman was the only congressional leader to object to the tactics being proposed. It is of note that in a 2007 report by investigator Dick Marty on secret CIA prisons, the phrase "enhanced interrogations" was stated to be a euphemism for torture. The documents show that top U.S. Officials were intimately involved in the discussion and approval of the harsher interrogation techniques used on Abu Zubaydah.

Condoleezza Rice ultimately told the CIA the harsher interrogation tactics were acceptable, In 2009 Rice stated, "We never tortured anyone." And Dick Cheney stated "I signed off on it; so did others." In 2010, Cheney remained unrepentant, saying, "I was and remain a strong proponent of our enhanced interrogation program." Pressed on his personal view of waterboarding, Karl Rove told the BBC in 2010: “I’m proud that we kept the world safer than it was, by the use of these techniques. They’re appropriate, they’re in conformity with our international requirements and with US law.” During the discussions John Ashcroft is reported as saying “Why are we talking about this in the White House? History will not judge this kindly.”

At least one adviser to Condoleezza Rice, Philip Zelikow, opposed the new, harsher interrogation techniques. Upon reading the August 1, 2002 memo which justified the torture, Zelikow authored his own memo contesting the Justice Department's conclusions, believing them wrong both legally and as a matter of policy. The Bush Administration attempted to collect all of the copies of Zelikow's memo and destroy them. Jane Mayer, author of the *Dark Side*, quotes Zelikow as predicting that "America's descent into torture will in time be viewed like the Japanese internments," in that "(f)ear and anxiety were exploited by zealots and fools."

Initial reports and complaints

Senior law enforcement agents with the Criminal Investigation Task Force told MSNBC.com in 2006 that they began to complain inside the U.S. Department of Defense in 2002 that the interrogation tactics used in Guantanamo Bay by a separate team of military intelligence investigators were unproductive, not likely to produce reliable information, and probably illegal. Unable to get satisfaction from the army commanders running the detainee camp, they took their concerns to David Brant, director of the Naval Criminal Investigative Service (NCIS), who alerted Navy General Counsel Alberto J. Mora.

General Counsel Mora and Navy Judge Advocate General Michael Lohr believed the detainee treatment to be unlawful, and campaigned among other top lawyers and officials in the Defense Department to investigate, and to provide clear standards prohibiting coercive interrogation tactics. In response, on January 15, 2003, Rumsfeld suspended the approved interrogation tactics at Guantánamo Bay until a new set of guidelines could be produced by a working group headed by General Counsel of the Air Force Mary Walker. The working group based its new guidelines on a legal memo from the United States Department of Justice Office of Legal Counsel written by John Yoo and signed by Jay S. Bybee, which would later become widely known as the "Torture Memo." General Counsel Mora led a faction of the Working Group in arguing against these standards, and argued the issues with Yoo in person. The working group's final report was signed and delivered to Guantánamo without the knowledge of Mora and the others who had opposed its content. Nonetheless, Mora has maintained that detainee treatment has been consistent with the law since the January 15, 2003 suspension of previously approved interrogation tactics.

Public positions and reactions

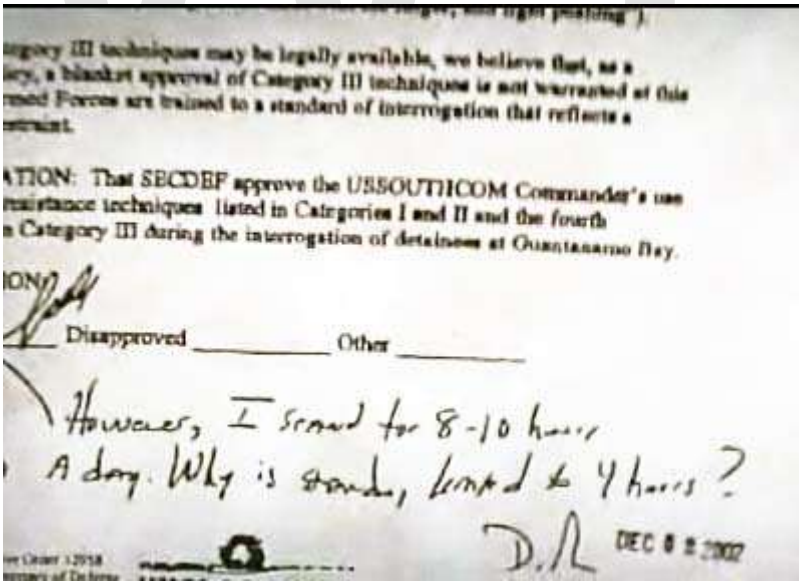
Official position of the Bush Administration

President Bush stated "The United States of America does not torture. And that's important for people around the world to understand."The administration adopted the Detainee Treatment Act of 2005 to address the multitude of incidents of detainee abuse. However, in his signing statement, Bush made clear that he reserved the right to waive this bill if he thought that was needed.

The *Washington Post* reported in January 2009 that Susan J. Crawford, convening authority of military commissions, stated in response to the interrogation of Mohammed al-Qahtani, the so-called "20th hijacker" of the September 11 attacks:

"The techniques they used were all authorized, but the manner in which they applied them was overly aggressive and too persistent.... You think of torture, you think of some horrendous physical act done to an individual. This was not any one particular act; this was just a combination of things that had a medical impact on him, that hurt his health. It was abusive and uncalled for. And coercive. Clearly coercive. It was that medical impact that pushed me over the edge", i.e., to call it torture.

The reason Crawford decided not to prosecute al-Qahtani was because his treatment fell within the definition of torture.



Comment from Donald Rumsfeld: "I stand for 8-10 hours a day. Why is standing by prisoners limited to four hours?"

According to the February 16, 2008 edition of *The Economist*, Rumsfeld also wrote in a 2002 memo; "I stand for 8-10 hours a day. Why is standing (by prisoners) limited to four

hours?" There have been no comments from either the Pentagon or US army spokespeople in Iraq on Karpinski's accusations.

Debates about whether "enhanced interrogation" constitutes torture

Former President Bush in his published memoirs defends the utility of "enhanced interrogation" techniques and asserts that they are not torture.

However, President Obama, Attorney General Holder, and Guantanamo military prosecutor Crawford called the techniques torture. The British government has determined the techniques would be classified as torture, and dismissed President Bush's claim to the contrary. A report byHuman Rights First (HRF) and Physicians for Human Rights (PFH) stated that these techniques constitute torture. They also cite the U.S. Office of the Inspector General report which concluded that "SERE-type interrogation techniques constitute 'physical or mental torture and coercion under the Geneva conventions.'" A United Nations report denounced the US abuse of prisoners as tantamount to torture. The UN report called for cessation of the US-termed "enhanced interrogation" techniques, as the UN sees these methods as a form of torture. The UN report also admonishes against secret prisons, the use of which, is considered to amount to torture as well and should be discontinued.

The US press has been hesitant to call enhanced interrogation torture because as Paul Kane of the *Washington Post* explained, torture is a crime and nobody who engaged in "enhanced interrogation" has been charged or convicted. *The New York Times* terms the techniques "harsh" and "brutal" while avoiding the word "torture" in most but not allnews articles, though it routinely calls "enhanced interrogation" torture in editorials.

Following NPR's controversial ban on using the word torture and Ombudsman Alica Shepard's defense of the policy that "calling waterboarding torture is tantamount to taking sides", Berkeley Professor of Linguistics Geoffrey Nunbergpointed out that virtually all media around the world, other than what he called the "spineless U.S. media", call these techniques torture. In an article on the euphemisms invented by the media that also criticized NPR, Glenn Greenwald discussed the enabling "corruption of American journalism":

This active media complicity in concealing that our Government created a systematic torture regime, by refusing ever to say so, is one of the principal reasons it was allowed to happen for so long. The steadfast, ongoing refusal of our leading media institutions to refer to what the Bush administration did as "torture" -- even in the face of more than 100 detainee deaths; the use of that term by a leading Bush official to describe what was done at Guantanamo; and the fact that media outlets frequently use the word "torture" to describe the exact same methods when used by other countries --reveals much about how the modern journalist thinks.

Atlantic Monthly writer Andrew Sullivan asserts the first use of a term comparable to "enhanced interrogation" was a 1937 memo byGestapoChief Heinrich Muller coining the

phrase "Verschärfte Vernehmung," German for (according to Sullivan) "sharpened," "intensified" or "enhanced interrogation" to describe subjection to extreme cold, sleep deprivation, and deliberate exhaustion among other techniques. Sullivan reports that in 1948 Norway prosecuted German officials for what trial documents termed "Verschärfte Vernehmung" including subjection to cold water, and repeated beatings. It is as yet unclear when US government officials first adopted the term enhanced interrogation, and there is no evidence they were aware of its antecedents in Gestapo terminology.

Debates concerning effectiveness or reliability of techniques

Also, according to the *New York Times*:

Experts advising the Bush administration on new interrogation rules warn that harsh techniques used since 2001 terrorist attacks are outmoded, amateurish and unreliable.

The Washington Post described the report by the Intelligence Science Board:

There is almost no scientific evidence to back up the U.S. intelligence community's use of controversial interrogation techniques in the fight against terrorism, and experts believe some painful and coercive approaches could hinder the ability to get good information, according to a new report from an intelligence advisory group.

The so-called ticking time bomb scenario is frequently used to justify extreme interrogation. Michael Chertoff, the Homeland Security Chief under Bush, declared that *24* "reflects real life", John Yoo, the former Justice Department lawyer who produced the torture memos cited Bauer in support while Supreme Court Justice Antonin Scalia went farther, *"Jack Bauer saved Los Angeles... He saved hundreds of thousands of lives. Are you going to convict Jack Bauer?"*; however, 24 is fictional and these situations only arise on television. Dick Cheney stated: "I know specifically of reports... that lay out what we learnt through the interrogation process and what the consequences were for the country", yet the only examples publicly released are the claim that the waterboarding of Khalid Shaikh Mohammed helped prevent a planned attack on Los Angeles in 2002, overlooking that he wasn't captured until 2003 and that of Ibn al-Shaykh al-Libi who had confessed that Iraq had trained al Qaeda in the use of weapons of mass destruction which was then used as justification for the subsequent invasion of Iraq, a confession now known to be false.

An academic analysis by Professor Shane O'Mara of the Trinity College Institute of Neuroscience concluded that "Prolonged stress from the CIA's harsh interrogations could have impaired the memories of terrorist suspects, diminishing their ability to recall and provide the detailed information the spy agency sought".

Former *Washington Post* writer Peter Carlson notes that when it became known U.S. troops were waterboarding Filipino guerrilla fighters in 1898, author Mark Twain remarked,

"To make him confess what? Truth? Or lies? How can one know which it is they are telling? For under unendurable pain a man confesses anything that is required of him, true or false, and his evidence is worthless."

Destruction of videotapes

In December 2007 it became known that the CIA had destroyed videotapes depicting prisoners being interrogated. Subsequent disclosures in 2010 revealed that Jose Rodriguez Jr., head of the directorate of operations at the CIA from 2004 to 2007, ordered the tapes destroyed because what they showed was so horrific they would be "devasting to the CIA," and that "the heat from destroying is nothing compared to what it would be if the tapes ever got into public domain." The *New York Times* reported that according to "some insiders" an inquiry into the C.I.A.'s secret detention program which analysed these techniques "might end with criminal charges for abusive interrogations." In an Op-ed for the New York Times Tom Kean and Lee Hamilton, chair and vice chair of the 9/11 Commission stated:

As a legal matter, it is not up to us to examine the C.I.A.'s failure to disclose the existence of these tapes. That is for others. What we do know is that government officials decided not to inform a lawfully constituted body, created by Congress and the president, to investigate one the greatest tragedies to confront this country. We call that obstruction.

Responding to the so-called "torture memoranda" Scott Horton pointed out

the possibility that the authors of these memoranda counseled the use of lethal and unlawful techniques, and therefore face criminal culpability themselves. That, after all, is the teaching of United States v. Altstötter, the Nuremberg case brought against German Justice Department lawyers whose memoranda crafted the basis for implementation of the infamous "Night and Fog Decree."

Jordan Paust concurred by responding to Mukasey's refusal to investigate and/or prosecute anyone that relied on these legal opinions

it is legally and morally impossible for any member of the executive branch to be acting lawfully or within the scope of his or her authority while following OLC opinions that are manifestly inconsistent with or violative of the law. General Mukasey, just following orders is no defense!

March 2009: ICRC report publicly reported

On March 15, 2009, Mark Danner provided a report in the *New York Review of Books* (with an abridged version in the *New York Times*) describing and commenting on the contents of a report by the International Committee of the Red Cross (ICRC), *Report on the Treatment of Fourteen "High Value Detainees" in CIA Custody* (43 pp., February 2007). *Report...* is a record of interviews with black site detainees, conducted between October 6 and 11 and December 4 and 14, 2006, after their transfer to Guantánamo.

(According to Danner, the report was marked "confidential" and was not previously made public before being made available to him.)

Danner provides excerpts of interviews with detainees, including Abu Zubaydah, Walid bin Attash, and Khalid Shaikh Mohammed. According to Danner, the report contains sections on "methods of ill-treatment" including suffocation by water, prolonged stress standing, beatings by use of a collar, beating and kicking, confinement in a box, prolonged nudity, sleep deprivation and use of loud music, exposure to cold temperature/cold water, prolonged use of handcuffs and shackles, threats, forced shaving, and deprivation/restricted provision of solid food. Danner quotes the ICRC report as saying that, "in many cases, the ill-treatment to which they were subjected while held in the CIA program, either singly or in combination, constituted torture. In addition, many other elements of the ill-treatment, either singly or in combination, constituted cruel, inhuman or degrading treatment."

Investigation of enhanced interrogation techniques and calls for prosecution

Request for Special Counsel Probe of Harsh Interrogation Tactics

On June 8, 2008, fifty-six House Democrats asked for an independent investigation, raising the possibility that authorising these techniques may constitute a crime by Bush administration officials. The congressmen involved in calling for such an investigation included John Conyers, Jan Schakowsky, and Jerrold Nadler.

The letter was addressed to Attorney General Michael B. Mukasey observing that:

"... information indicates that the Bush administration may have systematically implemented, from the top down, detainee interrogation policies that constitute torture or otherwise violate the law."

The letter continues to state:

"Because these apparent 'enhanced interrogation techniques' were used under cover of Justice Department legal opinions, the need for an outside special prosecutor is obvious."

According to the Washington Post the request was denied because Attorney General Michael B. Mukasey felt that:

officials acted in "good faith" when they sought legal opinions, and that the lawyers who provided them used their best judgment.

The article also reported that:

He warned that criminalizing the process could cause policymakers to second-guess themselves and "harm our national security well into the future."

After Cheney acknowledged his involvement in authorising these tactics Senator Carl Levin, chair of the Armed Services Committee, a New York Times editorial, Glenn Greenwald and Scott Horton stressed the importance of a criminal investigation:

A prosecutor should be appointed to consider criminal charges against top officials at the Pentagon and others involved in planning the abuse.

International calls on Obama to investigate and prosecute

Shortly before the end of Bush's second term newsmedia in other countries were opining that under the United Nations Convention Against Torture the US is obligated to hold those responsible to account under criminal law.

The United Nations Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment -Professor Manfred Nowak- on January 20, 2008 remarked on German television that, following the inauguration of Barack Obama as new President, George W. Bush has lost his head of state immunity and under international law the U.S. is now mandated to start criminal proceedings against all those involved in these violations of the UN Convention Against Torture. Law professor Dietmar Herz explained Novak's comments by saying that under U.S. and international law former President Bush is criminally responsible for adopting torture as interrogation tool.

Preventing UK courts to investigate

On February 4, 2009 the British High Court ruled that evidence of possible torture in the case of Binyam Mohamed, an Ethiopian-born British resident who is held in Guantanamo Bay, could not be disclosed:

as a result of a statement by David Miliband, the foreign secretary, that if the evidence was disclosed the US would stop sharing intelligence with Britain. That would directly threaten the UK's national security, Miliband had told the court.

Responding to the ruling, David Davis, the Conservative MP and former shadow home secretary, commented:

The ruling implies that torture has taken place in the [Binyam] Mohamed case, that British agencies may have been complicit, and further, that the United States government has threatened our high court that if it releases this information the US government will withdraw its intelligence cooperation with the United Kingdom.

The High Court judges also stated that a criminal investigation, by the UK's attorney general, into possible torture has begun.

Legality

After the disclosure of the use of the techniques, debates arose over the legality of the techniques—whether or not they had violated U.S. or international law.

US governmental legal opinions

John Yoo, author of the "torture memos"

Following the September 11 attacks in 2001, several memoranda analyzing the legality of various interrogation methods were written by John Yoo from Office of Legal Counsel. The memos, known today as the "torture memos," advocate enhanced interrogation techniques, while pointing out that avoiding the Geneva Conventions would reduce the possibility of prosecution under the US War Crimes Act of 1996 for actions taken in the War on Terror. In addition, a new US definition of torture was issued. Most actions that fall under the international definition do not fall within this new definition advocated by the U.S.

The Bush administration told the CIA in 2002 that its interrogators working abroad would not violate US prohibitions against torture unless they "have the specific intent to inflict severe pain or suffering", according to a previously secret US Justice Department memo released on July 24, 2008. The interrogator's "good faith" and "honest belief" that the interrogation will not cause such suffering protects the interrogator, the memo adds. "Because specific intent is an element of the offense, the absence of specific intent negates the charge of torture", Jay Bybee, then the Assistant Attorney General, wrote in the memo dated August 1, 2002. The 18-page memo is heavily redacted, with 10 of its 18 pages completely blacked out and only a few paragraphs legible on the others.

Another memo released on the same day advises that "the waterboard," does "not violate the Torture Statute." It also cites a number of warnings against torture, including statements by President Bush and a then-new Supreme Court ruling "which raises possible concerns about future US judicial review of the [interrogation] Program."

A third memo instructs interrogators to keep records of sessions in which "enhanced interrogation techniques" are used. The memo is signed by then-CIA director George Tenet and dated January 28, 2003.

The memos were made public by the American Civil Liberties Union, which obtained the three CIA-related documents under Freedom of Information Act requests.

The less redacted version of the August 1, 2002 memo signed by Assistant Attorney General Jay Bybee (regarding Abu Zubaydah) and four memos from 2005 signed by Principal Deputy Assistant Attorney General Steven Bradbury addressed to CIA and analysing the legality of various specific interrogation methods, including waterboarding, were released by Barack Obama administration on April 16, 2009

Following the release of the CIA documents and now released from non disclosure agreements he had signed Philip Zelikow, a former State Department lawyer and adviser to then-Secretary of State Condoleezza Rice, stated that he had argued it was unlikely that "*any federal court would agree (that the approval of harsh interrogation techniques) ... was a reasonable interpretation of the Constitution.*" He was told to destroy copies of his own memo and claimed that the Bush Administration had ordered that other dissenting legal advice be collected and destroyed.

US Supreme Court Justice Antonin Scalia said on BBC Radio 4 that since these methods are not intended to punish they do not violate the Eighth Amendment to the United States Constitution, barring "cruel and unusual punishment", and as such may not be unconstitutional.

The US Supreme Court ruled in Hamdan v. Rumsfeld that, contrary to what the Bush administration advocated, Common Article 3 of the Geneva Conventions applies to all detainees in the war on terrorism and as such the Military Tribunals used to try suspects were violating the law. The Court reaffirmed that those involved in mistreatment of detainees violate US and international law.

Opinions of international legal bodies

On May 19, 2006, the UN Committee against Torture issued a report stating the U.S. should stop, what it concludes, is "ill-treatment" of detainees, since such treatment, according to the report, violates international law.

Opinions of human rights organizations

A report by Human Rights First (HRF) and Physicians for Human Rights (PFH) stated that these techniques constitute torture. Their press release said:

The report concludes that each of the ten tactics is likely to violate U.S. laws, including the War Crimes Act, the U.S. Torture Act, and the Detainee Treatment Act of 2005.

Ban on interrogation techniques

On December 14, 2005, the Detainee Treatment Act was passed into law, specifically clarifying that interrogations techniques be limited to those explicitly authorized by the Army Field Manual. On February 13, 2008 the US Senate, in a 51 to 45 vote, approved a bill limiting the number of techniques allowed to only "those interrogation techniques explicitly authorized by the 2006 Army Field Manual." The Washington Post stated:

The measure would effectively ban the use of simulated drowning, temperature extremes and other harsh tactics that the CIA used on al-Qaeda prisoners after the Sept. 11, 2001, attacks.

President George W. Bush has said in a BBC interview he would veto such a bill after previously signing an executive order that

allows "enhanced interrogation techniques" and may exempt the CIA from Common Article 3 of the Geneva Conventions.

On March 8, 2008 President Bush vetoed this bill. "Because the danger remains, we need to ensure our intelligence officials have all the tools they need to stop the terrorists," Bush said in his weekly radio address. "The bill Congress sent me would take away one of the most valuable tools in the war on terror - the CIA program to detain and question key terrorist leaders and operatives." Bush said that the methods used by the military are designed for interrogating "lawful combatants captured on the battlefield", not the "hardened terrorists" normally questioned by the CIA. "If we were to shut down this program and restrict the CIA to methods in the Field Manual, we could lose vital information from senior al Qaida terrorists, and that could cost American lives," Bush said.

Massachusetts senator Edward Kennedy described Bush's veto as "one of the most shameful acts of his presidency". He said, "Unless Congress overrides the veto, it will go

down in history as a flagrant insult to the rule of law and a serious stain on the good name of America in the eyes of the world."

According to Jane Mayer, during the transition period for then President-elect Barack Obama, his legal, intelligence, and national-security advisers had met at the CIA's headquarters in Langley to discuss "whether a ban on brutal interrogation practices would hurt their ability to gather intelligence," and among the consulted experts:

There was unanimity among Obama's expert advisers... that to change the practices would not in any material way affect the collection of intelligence.

On January 22, 2009 President Obama signed an executive order requiring the CIA to use only the 19 interrogation methods outlined in the United States Army Field Manual on interrogations "unless the Attorney General with appropriate consultation provides further guidance."

Chapter- 4

Forensic Techniques

Hair analysis

Hair analysis is the chemical analysis of a hair sample. Hair may be considered for retrospective purposes when blood and urine are no longer expected to contain a particular contaminant, typically a year or less. Its most widely accepted use is in the fields of forensic toxicology and, increasingly, environmental toxicology. Several alternative medicine fields also use various hair analyses for environmental toxicology but these uses are controversial, evolving and not standardized.

Use in forensic toxicology

Hair analysis can refer to the forensic technique of assessing a number of different characteristics of hairs in order to determine whether they have a common source; for example, comparing hair found at the scene of the crime with hair samples taken from a suspect.

Hair analysis is also used for the detection of many therapeutic drugs and recreational drugs, including cocaine, heroin, benzodiazepines and amphetamines. In this context, it has been reliably used to determine compliance with therapeutic drug regimes or to check the accuracy of a witness statement that an illicit drug has not been taken. Hair testing is an increasingly common method of assessment in substance misuse, particularly in legal proceedings, or in any situation where a subject may have decided not to tell the entire truth about his or her substance-using history.

In December 1995 the Society of Hair Testing was founded to promote the research in hair testing technologies in forensic, clinical and occupational sciences, to develop the international proficiency tests, to organize meetings and workshops and to encourage the scientific cooperation and exchanges among members. The Board of the Society of Hair Testing agreed upon the latest version of a Consensus in Sevilla, Spain, in 2004.

Drug test

Hair samples are increasingly being used to detect the presence of illegal drugs both by the state and also by private employers who test their employees. The advantages of hair

analysis include the non-invasiveness, low cost and the ability to measure a large number of, potentially interacting, toxic and biologically essential elements.

Literature

Pragst F., Balikova M.A.: State of the art in hair analysis for detection of drugs and alcohol abuse; Clinica Chimic Acta 370 2006 17-49.

Auwärter V.: Fettsäureethylester als Marker exzessiven Alkoholkonsums – Analytische Bestimmung im Haar und in Hautoberflächenlipiden mittels Headspace-Festphasenmikroextraktion und Gaschromatographie-Massenspektrometrie. Dissertation Humboldt-Universität Berlin 2006.

Pragst F., Auwärter V., Kiessling B., Dyes C.: Wipe-test and patch-test ror alcohol misuse based on the concentration ratio of fatty acid ethyl esters and squalen CFAEE/CSQ in skin surface lipids. Forensic Sci Int 2004; 143:77-86.

Use in environmental toxicology

Analysis of hair samples has many advantages as a preliminary screening method for the presence of toxic substances deleterious to health after exposures in air, dust, sediment, soil and water, food and toxins in the environment. The advantages of hair analysis include the non-invasiveness, low cost and the ability to measure a large number of, potentially interacting, toxic and biologically essential elements. *Hence, head hair analysis is now increasingly being used as a preliminary test to see whether individuals have absorbed poisons linked to behavioral or health problems.*

Use in detection of long term elemental effects

There appears to be genuine validity to the use of hair analysis in the measurement of life-long, or long-term heavy metal burden, if not the measurement of general elemental analysis. Several interesting studies including the analysis of Ludwig van Beethoven's hair have been conducted in conjunction with the National Institutes of Health, and Centers for Disease Control and Prevention to name a few.

A 1999 study on hair concentrations of calcium, iron, and zinc in pregnant women and effects of supplementation, it was concluded that "From the analyses, it was clear that hair concentrations of Ca, Fe, and Zn could reflect the effects of supplementation...Finally, it could be concluded that mineral element deficiencies might be convalesced by adequate compensations of mineral element nutrients."

Use in occupational, environmental and alternative medicine

Hair analysis has been used in occupational, environmental and some branches of alternative medicine as a method of investigation to assist screening and/or diagnosis. The hair is sampled, processed and analyzed, studying the levels of mineral and metals in

the hair sample. Using the results, as part of a proper examination or test protocol, practitioners screen for toxic exposure and heavy metal poisoning. Some advocates claim that they can also diagnose mineral deficiencies and that people with autism have unusual hair mineral contents. These uses are often controversial, and the American Medical Association states, "The AMA opposes chemical analysis of the hair as a determinant of the need for medical therapy and supports informing the American public and appropriate governmental agencies of this unproven practice and its potential for health care fraud."

Vein matching

Vein matching, also called **vascular technology**, is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin. Though used by the Federal Bureau of Investigation and the Central Intelligence Agency, this method of identification is still in development and has not yet been universally adopted by crime labs as it is not considered as reliable as more established techniques, such as fingerprinting. However, it can be used in conjunction with existing forensic data in support of a conclusion.

Commercial applications

Vascular/vein pattern recognition (VPR) technology has been developed commercially by Hitachi since 1997, in which light reflected by hemoglobin in a subject's blood vessels is recorded by a CCD camera behind a transparent surface. The data patterns are processed, compressed, and digitized for future biometric authentication of the subject. Finger scanning devices have been deployed for use in Japanese financial institutions, kiosks, and turnstiles. Mantra Softech marketed a device in South Asia that scans vein patterns in palms for attendance recording. Fujitsu developed a version that does not require direct physical contact with the vein scanner for improved hygiene in the use of electronic point of sale devices.

Computer security expert Bruce Schneier stated that a key advantage of vein patterns for biometric identification is the lack of a known method of forging a usable "dummy", as is possible with fingerprints.

Forensic identification

According to a 31,000-word investigative report published in January 2011 by Georgetown University faculty and students, U.S. federal investigators used photos from the video recording of the beheading of American journalist Daniel Pearl to match the veins on the visible areas of the perpetrator to that of captured al-Qaeda operative Khalid Sheikh Mohammed, notably a "bulging vein" running across his hand. The FBI and the CIA used the matching technique on Mohammed in 2004 and again in 2007. Officials

were concerned that his confession, which had been obtained though waterboarding, would not hold up in court and used vein matching evidence to bolster their case.

Audit regime

An **audit regime** is usually a rigorous set of forensic accounting methods that is used to detect fraud. It refers more generally however to any similar regime of verification of conformity to some standard, e.g. Kyoto Protocol, Cocoa Protocol, or some mandatory labelling scheme. Without such a regime, transparency is simply not attainable.

Most accounting reform includes strict audit measures to verify that new standards are met.

Financial privacy is often in direct conflict with the desire for any stricter audit regimes.

Characteristics of an effective audit regime include:

- harsh penalties for any misleading or fraudulent disclosures to the auditor that are strictly enforced
- publicly visible reports and definitions, e.g. for capital categories
- an incorruptible profession of auditors that adheres to strict ethical codes, and whose careers are permanently and irrevocably destroyed by any serious impropriety
- strict standards to declare conflict of interest, and rules to prevent competitive arrangements that tend to create such conflicts, e.g. not permitting the auditor to also act as a consultant on meeting the regime's requirements.

After major accounting scandals in the United States that became publicly visible in 2001 and 2002, and the controversies about various ways of claiming carbon credits under the Kyoto Protocol, there has been increasing attention paid to audit regimes in the English speaking world. This has often focused on bringing United States standards up to the level of much stricter United Kingdom or European Union standards, which are of more recent origins.

Rossmo's formula

Rossmo's formula is a geographic profiling formula to predict where a serial criminal lives. The formula was developed by criminologist Kim Rossmo.

Formula

Imagine a map with an overlaying grid of little squares named sectors. If this map is a raster image file on a computer, these sectors are pixels. A sector $S_{i,j}$ is the square on row i and column j, located at coordinates (X_i,Y_j). The following function gives the probability $p_{i,j}$ of the position of the serial criminal residing within a specific sector (or point) (X_i,Y_j):

$$p_{i,j} = k \sum_{n=1}^{(\text{total crimes})} \left[\underbrace{\frac{\phi}{(|X_i - x_n| + |Y_j - y_n|)^f}}_{1^{\text{st}}\text{ term}} + \underbrace{\frac{(1-\phi)(B^{g-f})}{(2B - |X_i - x_n| - |Y_j - y_n|)^g}}_{2^{\text{nd}}\text{ term}} \right], \quad \text{Where } (X_i \neq x_n) \wedge (Y_i \neq y_n)$$

Where:

$$\phi = \begin{cases} 1, & \text{if } (|X_i - x_n| + |Y_i - y_n|) > B \iff (X_n, Y_n) \in B \\ 0, & \text{else} \end{cases}$$

Here the summation is over past crimes located at coordinates (x_n,y_n). φ is a characteristic function that returns 0 when a point X_i,Y_j is an element of the buffer zone B (the neighborhood of a criminal residence that is swept out by a radius of B from its center). φ allows p to switch between the two terms. When φ = 0, then the 1st term is nullified, allowing the 2nd term to be used to calculate the $p_{i,j}$. When φ = 1, the 1st term is used to calculate $p_{i,j}$.

$|X_i - x_n| + |Y_i - y_n|$ is the Manhattan distance between a point (X_i,Y_j) and the nth crime site (x_n,y_n)

$p_{i,j}$ becomes undefined when the distance between a point (or pixel) is zero.

Explanation

The summation in the formula consists of two terms. The first term describes the idea of *decreasing probability with increasing distance*. The second term deals with the concept of a *buffer zone*. The variable φ is used to put more weight on one of the two ideas. The variable *B* describes the radius of the buffer zone. The constant *k* is empirically determined.

The main idea of the formula is that the probability of crimes first increases as one moves through the buffer zone away from the *hotzone*, but decreases afterwards. The variable *f* can be chosen so that it works best on data of past crimes. The same idea goes for the variable *g*.

The distance is calculated with the Manhattan distance formula.

Applications

The formula has been applied to fields other than forensics. Because of the buffer zone idea, the formula works well for studies concerning predatory animals such as white sharks.

This formula and math behind it were used in crime detecting in Pilot episode of TV-series Numb3rs.

Chapter- 5

Polymerase Chain Reaction (Forensic Technique)

A strip of eight PCR tubes, each containing a 100 µl reaction mixture

The **polymerase chain reaction** (**PCR**) is a scientific technique in molecular biology to amplify a single or a few copies of a piece of DNA across several orders of magnitude, generating thousands to millions of copies of a particular DNA sequence.

Developed in 1983 by Kary Mullis, PCR is now a common and often indispensable technique used in medical and biological research labs for a variety of applications. These include DNA cloning for sequencing, DNA-based phylogeny, or functional analysis of genes; the diagnosis of hereditary diseases; the identification of genetic fingerprints (used in forensic sciences and paternity testing); and the detection and diagnosis of infectious diseases. In 1993, Mullis was awarded the Nobel Prize in Chemistry for his work on PCR.

The method relies on thermal cycling, consisting of cycles of repeated heating and cooling of the reaction for DNA melting and enzymatic replication of the DNA. Primers (short DNA fragments) containing sequences complementary to the target region along with a DNA polymerase (after which the method is named) are key components to enable selective and repeated amplification. As PCR progresses, the DNA generated is itself used as a template for replication, setting in motion a chain reaction in which the DNA template is exponentially amplified. PCR can be extensively modified to perform a wide array of genetic manipulations.

Almost all PCR applications employ a heat-stable DNA polymerase, such as Taq polymerase, an enzyme originally isolated from the bacterium *Thermus aquaticus*. This DNA polymerase enzymatically assembles a new DNA strand from DNA building blocks, the nucleotides, by using single-stranded DNA as a template and DNA oligonucleotides (also called DNA primers), which are required for initiation of DNA synthesis. The vast majority of PCR methods use thermal cycling, i.e., alternately heating and cooling the PCR sample to a defined series of temperature steps. These thermal cycling steps are necessary first to physically separate the two strands in a DNA double helix at a high temperature in a process called DNA melting. At a lower temperature, each strand is then used as the template in DNA synthesis by the DNA polymerase to selectively amplify the target DNA. The selectivity of PCR results from the use of primers that are complementary to the DNA region targeted for amplification under specific thermal cycling conditions.

PCR principles and procedure

Figure 1a: A thermal cycler for PCR

Figure 1b: An older model three-temperature thermal cycler for PCR

PCR is used to amplify a specific region of a DNA strand (the DNA target). Most PCR methods typically amplify DNA fragments of up to ~10 kilo base pairs (kb), although some techniques allow for amplification of fragments up to 40 kb in size.

A basic PCR set up requires several components and reagents. These components include:

- *DNA template* that contains the DNA region (target) to be amplified.
- Two *primers* that are complementary to the 3' (three prime) ends of each of the sense and anti-sense strand of the DNA target.

- *Taq polymerase* or another DNA polymerase with a temperature optimum at around 70 °C.
- *Deoxynucleotide triphosphates* (dNTPs), the building blocks from which the DNA polymerases synthesizes a new DNA strand.
- *Buffer solution,* providing a suitable chemical environment for optimum activity and stability of the DNA polymerase.
- *Divalent cations,* magnesium or manganese ions; generally Mg^{2+} is used, but Mn^{2+} can be utilized for PCR-mediated DNA mutagenesis, as higher Mn^{2+} concentration increases the error rate during DNA synthesis
- *Monovalent cation* potassium ions.

The PCR is commonly carried out in a reaction volume of 10–200 µl in small reaction tubes (0.2–0.5 ml volumes) in a thermal cycler. The thermal cycler heats and cools the reaction tubes to achieve the temperatures required at each step of the reaction (see below). Many modern thermal cyclers make use of the Peltier effect which permits both heating and cooling of the block holding the PCR tubes simply by reversing the electric current. Thin-walled reaction tubes permit favorable thermal conductivity to allow for rapid thermal equilibration. Most thermal cyclers have heated lids to prevent condensation at the top of the reaction tube. Older thermocyclers lacking a heated lid require a layer of oil on top of the reaction mixture or a ball of wax inside the tube.

Procedure

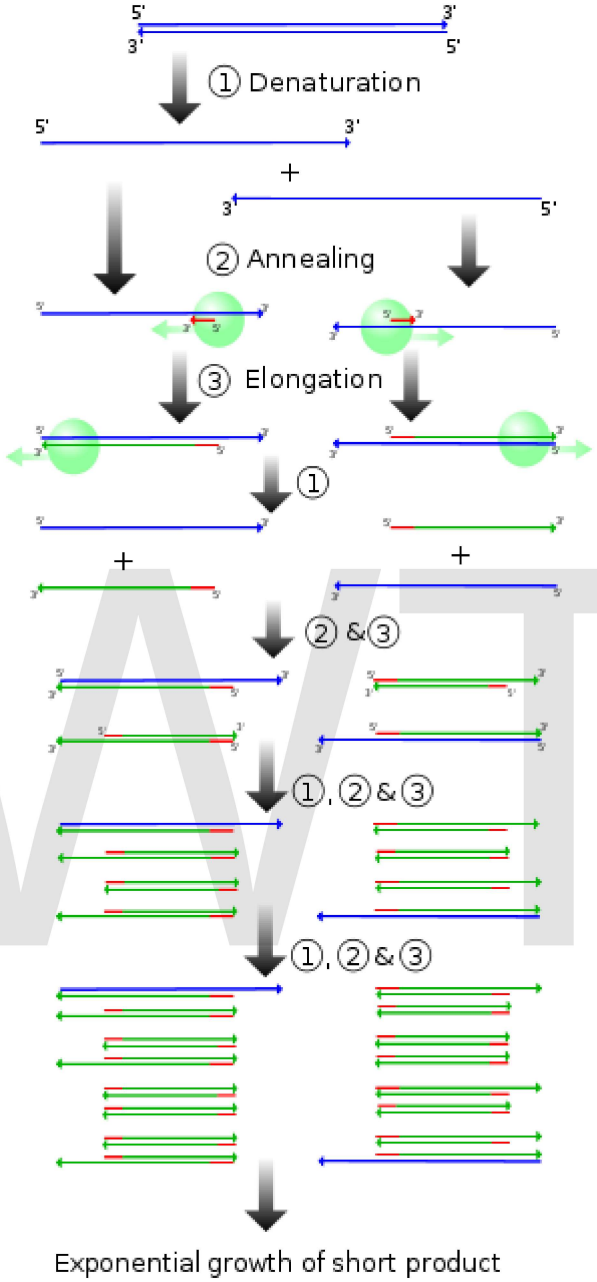


Figure 2: Schematic drawing of the PCR cycle. **(1) Denaturing at 94–96 °C. (2) Annealing at ~65 °C (3) Elongation at 72 °C**. Four cycles are shown here. The blue lines represent the DNA template to which primers (red arrows) anneal that are extended by the DNA polymerase (light green circles), to give shorter DNA products (green lines), which themselves are used as templates as PCR progresses.

Typically, PCR consists of a series of 20-40 repeated temperature changes, called cycles, with each cycle commonly consisting of 2-3 discrete temperature steps, usually three (Fig. 2). The cycling is often preceded by a single temperature step (called *hold*) at a high temperature (>90°C), and followed by one hold at the end for final product extension or brief storage. The temperatures used and the length of time they are applied in each cycle depend on a variety of parameters. These include the enzyme used for DNA synthesis, the concentration of divalent ions and dNTPs in the reaction, and the melting temperature (Tm) of the primers.

- *Initialization step*: This step consists of heating the reaction to a temperature of 94–96 °C (or 98 °C if extremely thermostable polymerases are used), which is held for 1–9 minutes. It is only required for DNA polymerases that require heat activation by hot-start PCR.

- *Denaturation step*: This step is the first regular cycling event and consists of heating the reaction to 94–98 °C for 20–30 seconds. It causes DNA melting of the DNA template by disrupting the hydrogen bonds between complementary bases, yielding single-stranded DNA molecules.

- *Annealing step*: The reaction temperature is lowered to 50–65 °C for 20–40 seconds allowing annealing of the primers to the single-stranded DNA template. Typically the annealing temperature is about 3-5 degrees Celsius below the Tm of the primers used. Stable DNA-DNA hydrogen bonds are only formed when the primer sequence very closely matches the template sequence. The polymerase binds to the primer-template hybrid and begins DNA synthesis.

- *Extension/elongation step*: The temperature at this step depends on the DNA polymerase used; Taq polymerase has its optimum activity temperature at 75–80 °C, and commonly a temperature of 72 °C is used with this enzyme. At this step the DNA polymerase synthesizes a new DNA strand complementary to the DNA template strand by adding dNTPs that are complementary to the template in 5' to 3' direction, condensing the 5'-phosphate group of the dNTPs with the 3'-hydroxyl group at the end of the nascent (extending) DNA strand. The extension time depends both on the DNA polymerase used and on the length of the DNA fragment to be amplified. As a rule-of-thumb, at its optimum temperature, the DNA polymerase will polymerize a thousand bases per minute. Under optimum conditions, i.e., if there are no limitations due to limiting substrates or reagents, at each extension step, the amount of DNA target is doubled, leading to exponential (geometric) amplification of the specific DNA fragment.

- *Final elongation*: This single step is occasionally performed at a temperature of 70–74 °C for 5–15 minutes after the last PCR cycle to ensure that any remaining single-stranded DNA is fully extended.

- *Final hold*: This step at 4–15 °C for an indefinite time may be employed for short-term storage of the reaction.

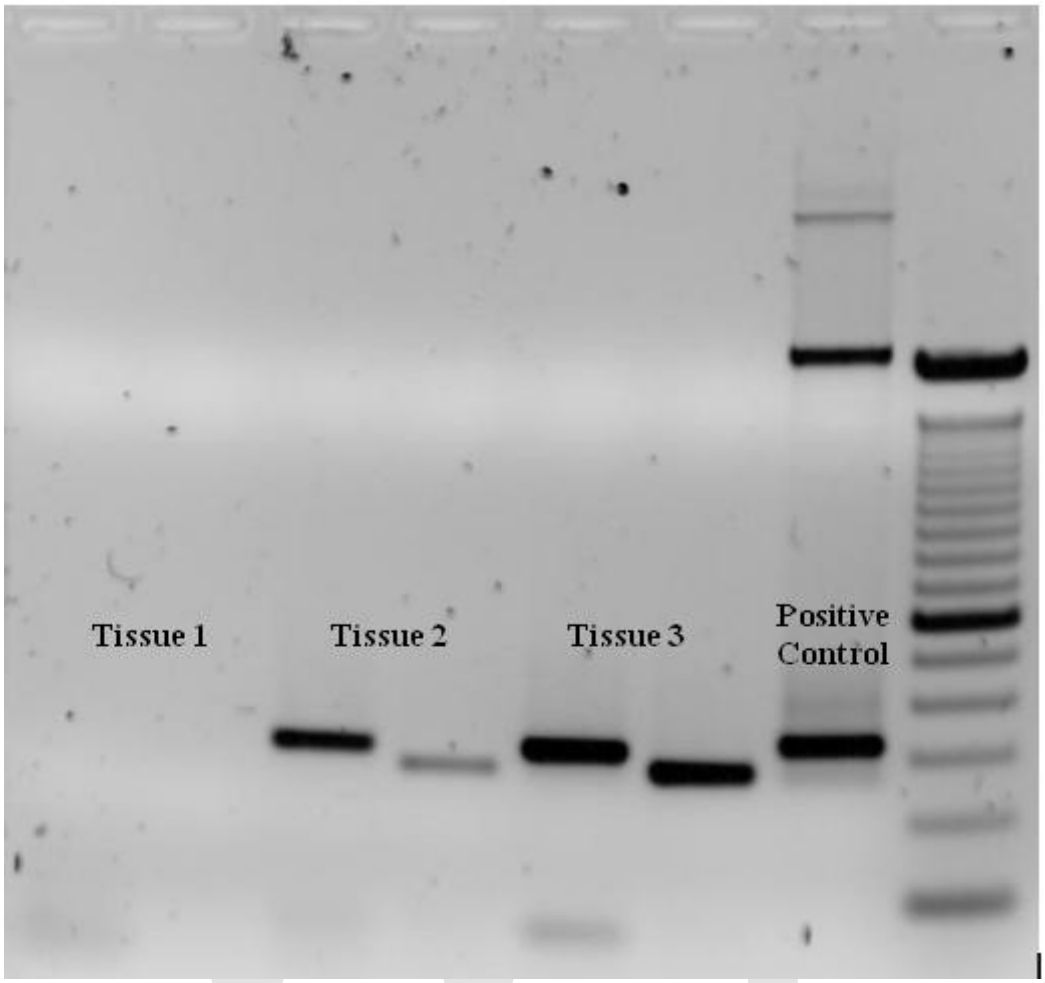


Figure 3: Ethidium bromide-stained PCR products after gel electrophoresis. Two sets of primers were used to amplify a target sequence from three different tissue samples. No amplification is present in sample #1; DNA bands in sample #2 and #3 indicate successful amplification of the target sequence. The gel also shows a positive control, and a DNA ladder containing DNA fragments of defined length for sizing the bands in the experimental PCRs.

To check whether the PCR generated the anticipated DNA fragment (also sometimes referred to as the amplimer or amplicon), agarose gel electrophoresis is employed for size separation of the PCR products. The size(s) of PCR products is determined by comparison with a DNA ladder (a molecular weight marker), which contains DNA fragments of known size, run on the gel alongside the PCR products (see Fig. 3).

PCR stages

The PCR process can be divided into three stages:

Exponential amplification: At every cycle, the amount of product is doubled (assuming 100% reaction efficiency). The reaction is very sensitive: only minute quantities of DNA need to be present.

Levelling off stage: The reaction slows as the DNA polymerase loses activity and as consumption of reagents such as dNTPs and primers causes them to become limiting.

Plateau: No more product accumulates due to exhaustion of reagents and enzyme.

PCR optimization

In practice, PCR can fail for various reasons, in part due to its sensitivity to contamination causing amplification of spurious DNA products. Because of this, a number of techniques and procedures have been developed for optimizing PCR conditions. Contamination with extraneous DNA is addressed with lab protocols and procedures that separate pre-PCR mixtures from potential DNA contaminants. This usually involves spatial separation of PCR-setup areas from areas for analysis or purification of PCR products, use of disposable plasticware, and thoroughly cleaning the work surface between reaction setups. Primer-design techniques are important in improving PCR product yield and in avoiding the formation of spurious products, and the usage of alternate buffer components or polymerase enzymes can help with amplification of long or otherwise problematic regions of DNA. Addition of reagents, such as formamide, in buffer systems may increase the specificity and yield of PCR.

Application of PCR

Selective DNA isolation

PCR allows isolation of DNA fragments from genomic DNA by selective amplification of a specific region of DNA. This use of PCR augments many methods, such as generating hybridization probes for Southern or northern hybridization and DNA cloning, which require larger amounts of DNA, representing a specific DNA region. PCR supplies these techniques with high amounts of pure DNA, enabling analysis of DNA samples even from very small amounts of starting material.

Other applications of PCR include DNA sequencing to determine unknown PCR-amplified sequences in which one of the amplification primers may be used in Sanger sequencing, isolation of a DNA sequence to expedite recombinant DNA technologies involving the insertion of a DNA sequence into a plasmid or the genetic material of another organism. Bacterial colonies (E. coli) can be rapidly screened by PCR for correct DNA vector constructs. PCR may also be used for genetic fingerprinting; a forensic technique used to identify a person or organism by comparing experimental DNAs through different PCR-based methods.

Some PCR 'fingerprints' methods have high discriminative power and can be used to identify genetic relationships between individuals, such as parent-child or between

siblings, and are used in paternity testing (Fig. 4). This technique may also be used to determine evolutionary relationships among organisms.

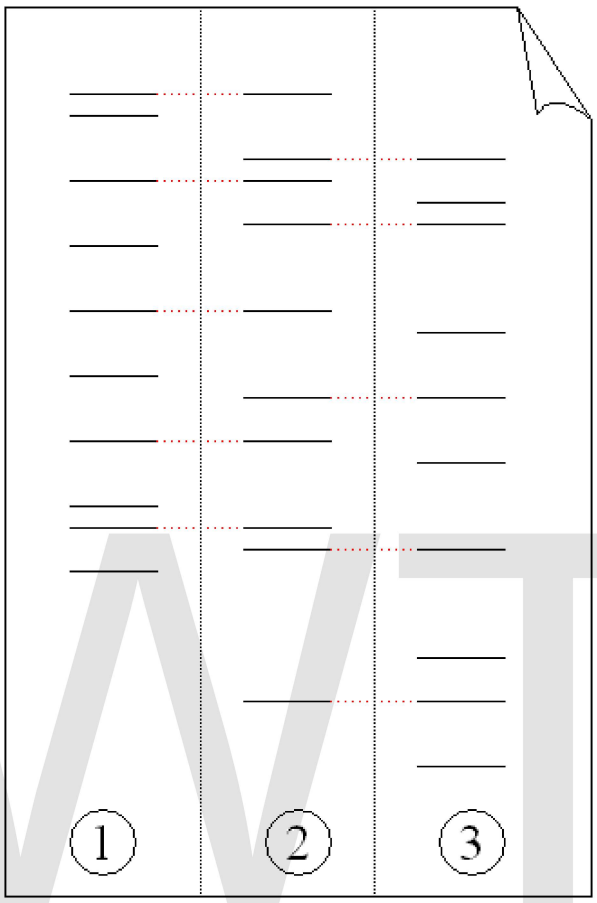


Figure 4: Electrophoresis of PCR-amplified DNA fragments. (1) Father. (2) Child. (3) Mother. The child has inherited some, but not all of the fingerprint of each of its parents, giving it a new, unique fingerprint.

Amplification and quantification of DNA

Because PCR amplifies the regions of DNA that it targets, PCR can be used to analyze extremely small amounts of sample. This is often critical for forensic analysis, when only a trace amount of DNA is available as evidence. PCR may also be used in the analysis of ancient DNA that is tens of thousands of years old. These PCR-based techniques have been successfully used on animals, such as a forty-thousand-year-old mammoth, and also on human DNA, in applications ranging from the analysis of Egyptian mummies to the identification of a Russian tsar.

Quantitative PCR methods allow the estimation of the amount of a given sequence present in a sample—a technique often applied to quantitatively determine levels of gene expression. Real-time PCR is an established tool for DNA quantification that measures the accumulation of DNA product after each round of PCR amplification.

PCR in diagnosis of diseases

PCR permits early diagnosis of malignant diseases such as leukemia and lymphomas, which is currently the highest developed in cancer research and is already being used routinely. PCR assays can be performed directly on genomic DNA samples to detect translocation-specific malignant cells at a sensitivity which is at least 10,000 fold higher than other methods.

PCR also permits identification of non-cultivatable or slow-growing microorganisms such as mycobacteria, anaerobic bacteria, or viruses from tissue culture assays and animal models. The basis for PCR diagnostic applications in microbiology is the detection of infectious agents and the discrimination of non-pathogenic from pathogenic strains by virtue of specific genes.

Viral DNA can likewise be detected by PCR. The primers used need to be specific to the targeted sequences in the DNA of a virus, and the PCR can be used for diagnostic analyses or DNA sequencing of the viral genome. The high sensitivity of PCR permits virus detection soon after infection and even before the onset of disease. Such early detection may give physicians a significant lead in treatment. The amount of virus ("viral load") in a patient can also be quantified by PCR-based DNA quantitation techniques (see below).

Variations on the basic PCR technique

- *Allele-specific PCR*: a diagnostic or cloning technique which is based on single-nucleotide polymorphisms (SNPs) (single-base differences in DNA). It requires prior knowledge of a DNA sequence, including differences between alleles, and uses primers whose 3' ends encompass the SNP. PCR amplification under stringent conditions is much less efficient in the presence of a mismatch between template and primer, so successful amplification with an SNP-specific primer signals presence of the specific SNP in a sequence.

- *Assembly PCR* or *Polymerase Cycling Assembly (PCA)*: artificial synthesis of long DNA sequences by performing PCR on a pool of long oligonucleotides with short overlapping segments. The oligonucleotides alternate between sense and antisense directions, and the overlapping segments determine the order of the PCR fragments, thereby selectively producing the final long DNA product.

- *Asymmetric PCR*: preferentially amplifies one DNA strand in a double-stranded DNA template. It is used in sequencing and hybridization probing where amplification of only one of the two complementary strands is required. PCR is carried out as usual, but with a great excess of the primer for the strand targeted for amplification. Because of the slow (arithmetic) amplification later in the reaction after the limiting primer has been used up, extra cycles of PCR are required. A recent modification on this process, known as *L*inear-*A*fter-*T*he-*E*xponential-PCR (LATE-PCR), uses a limiting primer with a higher melting

temperature (Tm) than the excess primer to maintain reaction efficiency as the limiting primer concentration decreases mid-reaction.

- *Helicase-dependent amplification*: similar to traditional PCR, but uses a constant temperature rather than cycling through denaturation and annealing/extension cycles. DNA helicase, an enzyme that unwinds DNA, is used in place of thermal denaturation.

- *Hot-start PCR*: a technique that reduces non-specific amplification during the initial set up stages of the PCR. It may be performed manually by heating the reaction components to the melting temperature (e.g., 95°C) before adding the polymerase. Specialized enzyme systems have been developed that inhibit the polymerase's activity at ambient temperature, either by the binding of an antibody or by the presence of covalently bound inhibitors that only dissociate after a high-temperature activation step. Hot-start/cold-finish PCR is achieved with new hybrid polymerases that are inactive at ambient temperature and are instantly activated at elongation temperature.

- *Intersequence-specific PCR* (ISSR): a PCR method for DNA fingerprinting that amplifies regions between simple sequence repeats to produce a unique fingerprint of amplified fragment lengths.

- *Inverse PCR*: is commonly used to identify the flanking sequences around genomic inserts. It involves a series of DNA digestions and self ligation, resulting in known sequences at either end of the unknown sequence.

- *Ligation-mediated PCR*: uses small DNA linkers ligated to the DNA of interest and multiple primers annealing to the DNA linkers; it has been used for DNA sequencing, genome walking, and DNA footprinting.

- *Methylation-specific PCR* (MSP): developed by Stephen Baylin and Jim Herman at the Johns Hopkins School of Medicine, and is used to detect methylation of CpG islands in genomic DNA. DNA is first treated with sodium bisulfite, which converts unmethylated cytosine bases to uracil, which is recognized by PCR primers as thymine. Two PCRs are then carried out on the modified DNA, using primer sets identical except at any CpG islands within the primer sequences. At these points, one primer set recognizes DNA with cytosines to amplify methylated DNA, and one set recognizes DNA with uracil or thymine to amplify unmethylated DNA. MSP using qPCR can also be performed to obtain quantitative rather than qualitative information about methylation.

- *Miniprimer PCR*: uses a thermostable polymerase (S-Tbr) that can extend from short primers ("smalligos") as short as 9 or 10 nucleotides. This method permits PCR targeting to smaller primer binding regions, and is used to amplify conserved DNA sequences, such as the 16S (or eukaryotic 18S) rRNA gene.

- *Multiplex Ligation-dependent Probe Amplification* (*MLPA*): permits multiple targets to be amplified with only a single primer pair, thus avoiding the resolution limitations of multiplex PCR (see below).

- *Multiplex-PCR*: consists of multiple primer sets within a single PCR mixture to produce amplicons of varying sizes that are specific to different DNA sequences. By targeting multiple genes at once, additional information may be gained from a single test run that otherwise would require several times the reagents and more time to perform. Annealing temperatures for each of the primer sets must be optimized to work correctly within a single reaction, and amplicon sizes, i.e., their base pair length, should be different enough to form distinct bands when visualized by gel electrophoresis.

- *Nested PCR*: increases the specificity of DNA amplification, by reducing background due to non-specific amplification of DNA. Two sets of primers are used in two successive PCRs. In the first reaction, one pair of primers is used to generate DNA products, which besides the intended target, may still consist of non-specifically amplified DNA fragments. The product(s) are then used in a second PCR with a set of primers whose binding sites are completely or partially different from and located 3' of each of the primers used in the first reaction. Nested PCR is often more successful in specifically amplifying long DNA fragments than conventional PCR, but it requires more detailed knowledge of the target sequences.

- *Overlap-extension PCR*: a genetic engineering technique allowing the construction of a DNA sequence with an alteration inserted beyond the limit of the longest practical primer length.

- *Quantitative PCR (Q-PCR)*: used to measure the quantity of a PCR product (commonly in real-time). It quantitatively measures starting amounts of DNA, cDNA or RNA. Q-PCR is commonly used to determine whether a DNA sequence is present in a sample and the number of its copies in the sample. *Quantitative real-time PCR* has a very high degree of precision. QRT-PCR methods use fluorescent dyes, such as Sybr Green, EvaGreen or fluorophore-containing DNA probes, such as TaqMan, to measure the amount of amplified product in real time. It is also sometimes abbreviated to RT-PCR (*R*eal *T*ime PCR) or RQ-PCR. QRT-PCR or RTQ-PCR are more appropriate contractions, since RT-PCR commonly refers to reverse transcription PCR (see below), often used in conjunction with Q-PCR.

- *R*everse *T*ranscription PCR (RT-PCR): for amplifying DNA from RNA. Reverse transcriptase reverse transcribes RNA into cDNA, which is then amplified by PCR. RT-PCR is widely used in expression profiling, to determine the expression of a gene or to identify the sequence of an RNA transcript, including transcription start and termination sites. If the genomic DNA sequence of a gene is known, RT-PCR can be used to map the location of exons and introns in the gene. The 5' end

of a gene (corresponding to the transcription start site) is typically identified by RACE-PCR (*Rapid Amplification of cDNA Ends*).

- *Solid Phase PCR*: encompasses multiple meanings, including Polony Amplification (where PCR colonies are derived in a gel matrix, for example), Bridge PCR (primers are covalently linked to a solid-support surface), conventional Solid Phase PCR (where Asymmetric PCR is applied in the presence of solid support bearing primer with sequence matching one of the aqueous primers) and Enhanced Solid Phase PCR (where conventional Solid Phase PCR can be improved by employing high Tm and nested solid support primer with optional application of a thermal 'step' to favour solid support priming).

- *Thermal asymmetric interlaced PCR (TAIL-PCR)*: for isolation of an unknown sequence flanking a known sequence. Within the known sequence, TAIL-PCR uses a nested pair of primers with differing annealing temperatures; a degenerate primer is used to amplify in the other direction from the unknown sequence.

- *Touchdown PCR* (*Step-down PCR*): a variant of PCR that aims to reduce nonspecific background by gradually lowering the annealing temperature as PCR cycling progresses. The annealing temperature at the initial cycles is usually a few degrees (3-5°C) above the T_m of the primers used, while at the later cycles, it is a few degrees (3-5°C) below the primer T_m. The higher temperatures give greater specificity for primer binding, and the lower temperatures permit more efficient amplification from the specific products formed during the initial cycles.

- *PAN-AC*: uses isothermal conditions for amplification, and may be used in living cells.

- *Universal Fast Walking*: for genome walking and genetic fingerprinting using a more specific 'two-sided' PCR than conventional 'one-sided' approaches (using only one gene-specific primer and one general primer - which can lead to artefactual 'noise') by virtue of a mechanism involving lariat structure formation. Streamlined derivatives of UFW are LaNe RAGE (lariat-dependent nested PCR for rapid amplification of genomic DNA ends), 5'RACE LaNe and 3'RACE LaNe.

History

A 1971 paper in the Journal of Molecular Biology by Kleppe and co-workers first described a method using an enzymatic assay to replicate a short DNA template with primers *in vitro*. However, this early manifestation of the basic PCR principle did not receive much attention, and the invention of the polymerase chain reaction in 1983 is generally credited to Kary Mullis.

At the core of the PCR method is the use of a suitable DNA polymerase able to withstand the high temperatures of >90 °C (194 °F) required for separation of the two DNA strands in the DNA double helix after each replication cycle. The DNA polymerases initially

employed for in vitro experiments presaging PCR were unable to withstand these high temperatures. So the early procedures for DNA replication were very inefficient, time consuming, and required large amounts of DNA polymerase and continual handling throughout the process.

The discovery in 1976 of Taq polymerase — a DNA polymerase purified from the thermophilic bacterium, *Thermus aquaticus*, which naturally lives in hot (50 to 80 °C (122 to 176 °F)) environments such as hot springs — paved the way for dramatic improvements of the PCR method. The DNA polymerase isolated from *T. aquaticus* is stable at high temperatures remaining active even after DNA denaturation, thus obviating the need to add new DNA polymerase after each cycle. This allowed an automated thermocycler-based process for DNA amplification.

When Mullis developed the PCR in 1983, he was working in Emeryville, California for Cetus Corporation, one of the first biotechnology companies. There, he was responsible for synthesizing short chains of DNA. Mullis has written that he conceived of PCR while cruising along the Pacific Coast Highway one night in his car. He was playing in his mind with a new way of analyzing changes (mutations) in DNA when he realized that he had instead invented a method of amplifying any DNA region through repeated cycles of duplication driven by DNA polymerase. In *Scientific American*, Mullis summarized the procedure: "Beginning with a single molecule of the genetic material DNA, the PCR can generate 100 billion similar molecules in an afternoon. The reaction is easy to execute. It requires no more than a test tube, a few simple reagents, and a source of heat." He was awarded the Nobel Prize in Chemistry in 1993 for his invention, seven years after he and his colleagues at Cetus first put his proposal to practice. However, some controversies have remained about the intellectual and practical contributions of other scientists to Mullis' work, and whether he had been the sole inventor of the PCR principle (see below).

Patent wars

The PCR technique was patented by Kary Mullis and assigned to Cetus Corporation, where Mullis worked when he invented the technique in 1983. The *Taq* polymerase enzyme was also covered by patents. There have been several high-profile lawsuits related to the technique, including an unsuccessful lawsuit brought by DuPont. The pharmaceutical company Hoffmann-La Roche purchased the rights to the patents in 1992 and currently holds those that are still protected.

A related patent battle over the Taq polymerase enzyme is still ongoing in several jurisdictions around the world between Roche and Promega. The legal arguments have extended beyond the lives of the original PCR and Taq polymerase patents, which expired on March 28, 2005.

Chapter- 6

Brain Fingerprinting

"Brain Fingerprinting" is exactly identical to standard P300 lie detection using David Lykken's "Guilty Knowledge Test", except that it also uses other brainwaves in addition to P300. Only one study--(Farwell & Smith 2001)--has ever tested its accuracy, and that laboratory study by "Brain Fingerprinting"'s developer used only 6 participants (3 "guilty" and 3 "innocent"), rendering any conclusions drawn therefrom statistically insignificant (psychologists typically require 3 sigma and n=15 for minimal statistical significance). The citations in the rest, particularly to the work of Iacono, are mis-attributed and refer to studies of the P300 GKT method alone, not to Farwell's "Brain Fingerprinting." P300 measurement of the GKT "orienting reflex" is as accurate as polygraph measurement of the orienting reflex, and there is no logical reason to believe (and no (good) scientific studies to demonstrate) that using other brainwaves in addition to P300 will improve the test, as the problem isn't measuring the physiological "orienting reflex" response but in formulating the right questions and alternatives for the situation.

Beware that what follows below is merely self-promotion by Farwell (and the accuracy rate (100%) is ridiculous and will never stand up to rigorous testing).

Brain Fingerprinting is a controversial forensic science technique that uses brain-reading techniques to determine whether specific information is stored in a subject's brain. It does this by measuring electrical brainwave responses to words, phrases, or pictures that are presented on a computer screen (Farwell & Smith 2001). Brain fingerprinting was invented by Lawrence Farwell. The theory is that the brain processes known, relevant information differently from the way it processes unknown or irrelevant information (Farwell & Donchin 1991). The brain's processing of known information, such as the details of a crime stored in the brain, is revealed by a specific pattern in the EEG (electroencephalograph) (Farwell & Smith 2001, Farwell 1994). Farwell's brain fingerprinting originally used the well known P300 brain response to detect the brain's recognition of the known information (Farwell & Donchin 1986, 1991; Farwell 1995a). Later Farwell discovered the MERMER ("Memory and Encoding Related Multifaceted Electroencephalographic Response"), which includes the P300 and additional features and is reported to provide a higher level of accuracy than the P300 alone (Farwell & Smith 2001, Farwell 1994, Farwell 1995b). In peer-reviewed publications Farwell and colleagues report over 99% accuracy in laboratory research (Farwell & Donchin 1991, Farwell & Richardson 2006) and real-life field applications (Farwell & Smith 2001, Farwell *et al.* 2006). In independent research William Iacono and others who followed

identical or similar scientific protocols to Farwell's have reported a similar high level of accuracy (e.g., Allen & Iacono 1997).

Brain fingerprinting has been applied in a number of high-profile criminal cases, including helping to catch serial killer JB Grinder (Dalbey 1999) and to exonerate innocent convict Terry Harrington after he had been falsely convicted of murder (Harrington v. State). Brain fingerprinting has been ruled admissible in court (Harrington v. State, Farwell & Makeig 2005). In the controversial Sister Abhaya murder case, the Ernakulam Chief Judicial Magistrate court had asked the Central Bureau of Investigation to make use of all modern investigation techniques, including brain fingerprinting.

Brain fingerprinting technique has been criticized on a number of fronts (Fox 2006b, Abdollah 2003). Although independent scientists who have used the same or similar methods as Farwell's brain fingerprinting have achieved similar, highly accurate results, different methods have yielded different results. J. Peter Rosenfeld used P300-based tests incorporating fundamentally different methods, resulting in as low as chance accuracy (Rosenfeld *et al.* 2004) as well as susceptibility to countermeasures, and criticized brain fingerprinting based on the premise that the shortcomings of his alternative technique should generalize to all other techniques in which the P300 is among the brain responses measured, including brain fingerprinting.

Brain Fingerprinting was an international finalist in the Global Security Challenge 2008 in London.

Technique

The technique uses the well known fact that an electrical signal known as P300 is emitted from an individual's brain beginning approximately 300 milliseconds after it is confronted with a stimulus of special significance, e.g. a rare vs. a common stimulus or a stimulus the subject is asked to count. The application of this in brain fingerprinting is to detect the P300 as a response to stimuli related to the crime or other investigated situation, e.g., a murder weapon, victim's face, or knowledge of the internal workings of a terrorist cell (Farwell 1992a, Farwell & Donchin 1991, Harrington v. State). Because it is based on EEG signals, the system does not require the subject to issue verbal responses to questions or stimuli.

The person to be tested wears a special headband with electronic sensors that measure the EEG from several locations on the scalp. The subject views stimuli consisting of words, phrases, or pictures presented on a computer screen. Stimuli are of three types: 1) "irrelevant" stimuli that are irrelevant to the investigated situation and to the test subject, 2) "target" stimuli that are relevant to the investigated situation and are known to the subject, and 3) "probe" stimuli that are relevant to the investigated situation and that the subject denies knowing. Probes contain information that is known only to the perpetrator and investigators, and not to the general public or to an innocent suspect who was not at the scene of the crime. Before the test, the scientist identifies the targets to the subject, and makes sure that he/she knows these relevant stimuli. The scientist also makes sure

that the subject does not know the probes for any reason unrelated to the crime, and that the subject denies knowing the probes. The subject is told why the probes are significant (e.g., “You will see several items, one of which is the murder weapon”), but is not told which items are the probes and which are irrelevant (Farwell 1994, Simon 2005).

Since brain fingerprinting uses cognitive brain responses, brain fingerprinting does not depend on the emotions of the subject, nor is it affected by emotional responses (Farwell & Smith 2001, Farwell 1992a, 1995a). Brain fingerprinting is fundamentally different from the polygraph (lie-detector), which measures emotion-based physiological signals such as heart rate, sweating, and blood pressure (Farwell 1994). Also, unlike polygraph testing, it does not attempt to determine whether or not the subject is lying or telling the truth. Rather, it measures the subject’s brain response to relevant words, phrases, or pictures to detect whether or not the relevant information is stored in the subject’s brain (Farwell & Smith 2001, Simon 2005, Harrington v. State).

By comparing the responses to the different types of stimuli, the brain fingerprinting system mathematically computes a determination of “information present” (the subject knows the crime-relevant information contained in the probe stimuli) or “information absent” (the subject does not know the information) and a statistical confidence for the determination. This determination is mathematically computed, and does not involve the subjective judgment of the scientist.

Background and terminology

"Brain fingerprinting" is a computer-based test that is designed to discover, document, and provide evidence of guilty knowledge regarding crimes, and to identify individuals with a specific training or expertise such as members of dormant terrorist cells or bomb makers. It has also been used to evaluate brain functioning as a means of early detection of Alzheimer’s and other cognitively degenerative diseases, and to evaluate the effectiveness of advertising by measuring brain responses.

The technique is described in Dr. Farwell's paper “Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal”, published in the Journal of Forensic Sciences in 2001 by Dr. Farwell and FBI Supervisory Special Agent Sharon Smith of the FBI (Farwell & Smith 2001).

The paper describes a test of brain fingerprinting, a technology based on EEG that is purported to be able to detect the existence of prior knowledge or memory in the brain. The P300 occurs when the tested subject is presented with a rarely occurring stimulus that is significant in context (for example, in the context of a crime) (Gaillard & Ritter 1983, Farwell & Donchin 1991). When an irrelevant stimulus is presented, a P300 is not expected to occur (Picton 1988, Farwell & Donchin 1991, Farwell & Smith 2001). The P300 is widely known in the scientific community, and is also known as an oddball-evoked P300.

While researching the P300, Dr. Farwell created a more detailed test that not only includes the P300, but also observes the stimulus response up to 1400 ms after the stimulus. He calls this brain response a MERMER, memory and encoding related multifaceted electroencephalographic response. The P300, an electrically positive component, is maximal at the midline parietal area of the head and has a peak latency of approximately 300 to 800 ms. The MERMER includes the P300 and also includes an electrically negative component, with an onset latency of approximately 800-1200ms (Farwell 1994, Farwell & Smith 2001). According to Dr. Farwell, the MERMER includes additional features involving changes in the frequency of the EEG signal, but for the purposes of signal detection and practical application the MERMER is sufficiently characterized by the P300 and the following negative component in the brain response (Farwell 1994, Farwell & Smith 2001, Farwell *et al.* 2006).

Current uses and research

Brain Fingerprinting has two primary applications: 1) detecting the record of a specific crime, terrorist act, or incident stored in the brain (Farwell & Smith 2001, Dalbey 1999), and 2) detecting a specific type of knowledge, expertise, or training, such as knowledge specific to FBI agents, Al-Qaeda -trained terrorists, or bomb makers (Farwell 1992b, Farwell 1993, Farwell *et al.* 2006).

The seminal paper by Dr. Farwell and Emmanuel Donchin (Farwell & Donchin 1991) reported successful application of the technique in detecting knowledge of both laboratory mock crimes and real-life events, with no false positives and no false negatives.

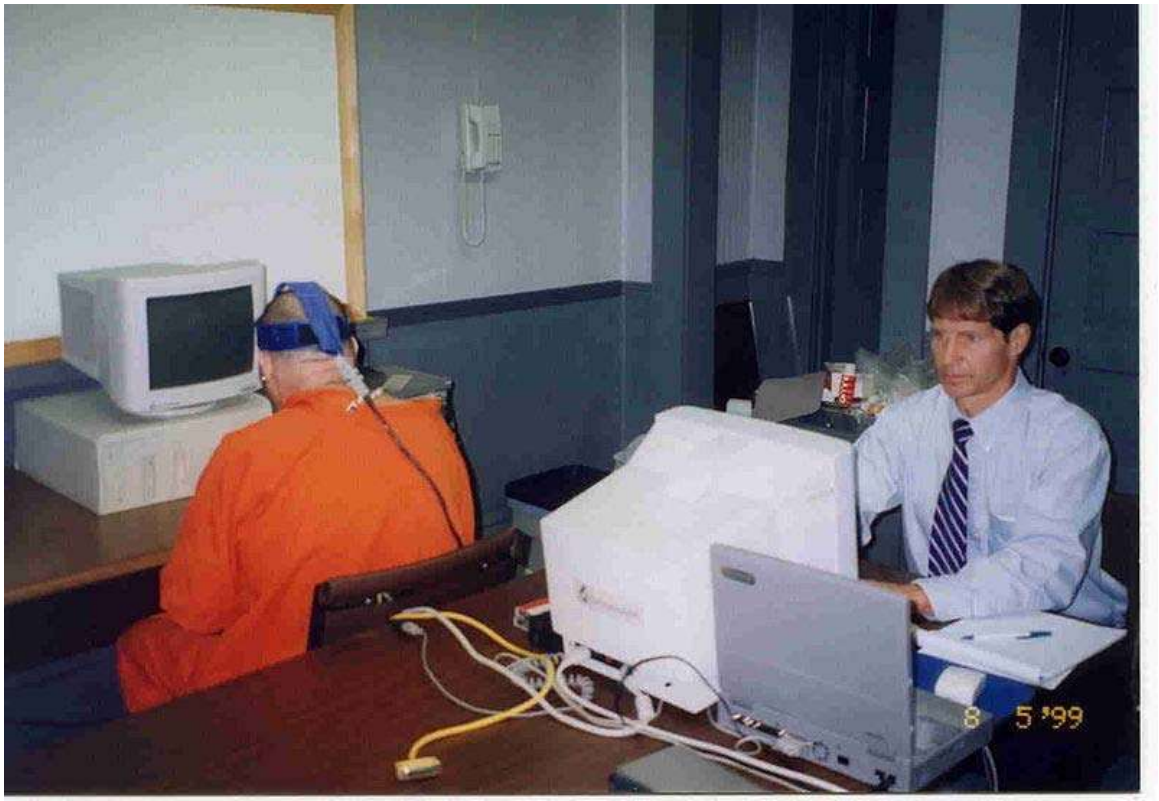
In a study with the FBI, Dr. Farwell and FBI scientist Drew Richardson, former chief of the FBI's chem-bio-nuclear counterterrorism unit, used brain fingerprinting to show that test subjects from specific groups could be identified by detecting specific knowledge which would only be known to members of those groups (Farwell 1993, Farwell *et al.* 2006). A group of 17 FBI agents and 4 non-agents were exposed to stimuli (words, phrases, and acronyms) that were flashed on a computer screen. The probe stimuli contained information that would be common knowledge only to someone with FBI training. Brain fingerprinting correctly distinguished the FBI agents from the non-agents.

The CIA has also funded Farwell's research (Dale 2001). In a study funded by the CIA, Farwell and colleagues (Farwell *et al.* 2006) used brain fingerprinting to detect which individuals had US Navy military medical training. All 30 subjects were correctly determined to have or not to have the specific information regarding military medicine stored in their brains. In another CIA-funded study, brain fingerprinting correctly detected which individuals had participated in specific real-life events, some of which were crimes, based on the record stored in their brains. Accuracy again was 100% (Farwell *et al.* 2006). Dr. Farwell collaborated with FBI scientist Sharon Smith in a further study in which brain fingerprinting detected real-life events that was published in the *Journal of Forensic Sciences* (Farwell & Smith 2001).

In another CIA-funded study, a group of subjects enacted a simulated espionage scenario and were then tested on relevant stimuli in the form of pictorial probes. Brain fingerprinting correctly identified all individuals who were "information present" and "information absent" (Farwell & Richardson 2006).

Use in criminal investigation

Dr. Lawrence Farwell conducts a Brain Fingerprinting test on Terry Harrington



Dr. Lawrence Farwell conducts a Brain Fingerprinting test on serial killer JB Grinder

Farwell's brain fingerprinting has been ruled admissible as evidence in court in the reversal of the murder conviction of Terry Harrington (Harrington v. State, Farwell & Makeig 2005). Following a hearing on post-conviction relief on November 14, 2000, an Iowa District Court held that Dr. Farwell's brain fingerprinting P-300 test results were admissible as scientific evidence as defined in Congress Ruling 702 and in the Daubert standard. Harrington was freed by the Iowa Supreme Court on grounds.

Based on two days of testimony from expert witnesses on both sides of the issue and hundreds of pages of supporting documentation, brain fingerprinting was ruled admissible in the Harrington case (Harrington v. State). In order to be ruled admissible under the prevailing Daubert standard established by the US Supreme Court, the Court required proof that brain fingerprinting is 1) tested and proven, 2) peer reviewed and published, 3) accurate and systematically applied, and 4) well accepted in the relevant scientific community. In ruling brain fingerprinting admissible as scientific evidence, the Court stated the following:

"In the spring of 2000, Harrington was given a test by Dr. Lawrence Farwell. The test is based on a 'P300 effect'."

"The P-300 effect has been recognized for nearly twenty years."

"The P-300 effect has been subject to testing and peer review in the scientific community."

"The consensus in the community of psycho-physiologists is that the P300 effect is valid."

“The evidence resulting from Harrington’s ‘brain fingerprinting’ test was discovered after the fact. It is newly discovered.”

(Harrington v. State)

Brain Fingerprinting testing was also “instrumental in obtaining a confession and guilty plea” from serial killer James B. Grinder, according to Sheriff Robert Dawson of Macon County, Missouri. In August 1999 Dr. Farwell conducted a brain fingerprinting test on Grinder, showing that information stored in his brain matched the details of the murder of Julie Helton (Dalbey 1999). Faced with a certain conviction and almost certain death sentence, Grinder then pled guilty to the rape and murder of Julie Helton in exchange for a life sentence without parole. He is currently serving that sentence and has also confessed to the murders of three other women.

Limitations of brain fingerprinting

Both the strengths and limitations of brain fingerprinting are documented in detail in the expert witness testimony of Dr. Farwell and two other expert witnesses in the Harrington case (Harrington v. State) and in a Law Enforcement Technology article (Simon 2005) as well as in Farwell’s publications and patents (e.g., Farwell 1994, Farwell 1995a, b, Farwell & Smith 2001). The limitations of brain fingerprinting described below are also summarized in PBS 2004, PBS Innovation Series – “Brain Fingerprinting: Ask the Experts”.

Brain fingerprinting detects information-processing brain responses that reveal what information is stored in the subject’s brain. It does not detect how that information got there. This fact has implications for how and when the technique can be applied. In a case where a suspect claims not to have been at the crime scene and has no legitimate reason for knowing the details of the crime, and investigators have information that has not been released to the public, brain fingerprinting can determine objectively whether or not the subject possesses that information. In such a case, brain fingerprinting could provide useful evidence.

If, however, the suspect knows everything that the investigators know about the crime for some legitimate reason, then the test cannot be applied. There are several circumstances in which this may be the case. If a suspect acknowledges being at the scene of the crime, but claims to be a witness and not a perpetrator, then the fact that he knows details about the crime would not be incriminating. There would be no reason to conduct a test, because the resulting “information present” response would simply show that the suspect

knew the details about the crime – knowledge which he already admits and which he gained at the crime scene whether he was a witness or a perpetrator.

Another case where brain fingerprinting is not applicable would be one wherein a suspect and an alleged victim – say, of an alleged sexual assault – agree on the details of what was said and done, but disagree on the intent of the parties. Brain fingerprinting detects only information, and not intent. The fact that the suspect knows the uncontested facts of the circumstance does not tell us which party's version of the intent is correct.

In a case where the suspect knows everything that the investigators know because he has been exposed to all available information in a previous trial, there is no available information with which to construct probe stimuli, so a test cannot be conducted. Even in a case where the suspect knows many of the details about the crime, however, it is sometimes possible to discover salient information that the perpetrator must have encountered in the course of committing the crime, but the suspect claims not to know and would not know if he were innocent. This was the case with Terry Harrington (Harrington v. State). By examining reports, interviewing witnesses, and visiting the crime scene and surrounding areas, Dr. Farwell was able to discover salient features of the crime that Harrington had never been exposed to at his previous trials. The brain fingerprinting test showed that the record in Harrington's brain did not contain these salient features of the crime, but only the details about the crime that he had learned after the fact.

Obviously, in structuring a brain fingerprinting test, a scientist must avoid including information that has been made public. Detecting that a suspect knows information he obtained by reading a newspaper would not be of use in a criminal investigation, and standard brain fingerprinting procedures eliminate all such information from the structuring of a test (Farwell 1995a, Simon 2005, Harrington v. State). News accounts containing many of the details of a crime do not interfere with the development of a brain fingerprinting test, however; they simply limit the material that can be tested. Even in highly publicized cases, there are almost always many details that are known to the investigators but not released to the public (Simon 2005), and these can be used as stimuli to test the subject for knowledge that he would have no way to know except by committing the crime.

Another situation where brain fingerprinting is not applicable is one where the authorities have no information about what crime may have taken place. For example, an individual may disappear under circumstances where a specific suspect had a strong motive to murder the individual. Without any evidence, authorities do not know whether a murder took place, or the individual decided to take a trip and tell no one, or some other criminal or non-criminal event happened. If there is no known information on which a suspect could be tested, a brain fingerprinting test cannot be structured.

Similarly, brain fingerprinting is not applicable for general screening, for example, in general pre-employment or employee screening wherein any number of undesirable activities or intentions may be relevant. If the investigators have no idea what crime or

undesirable act the individual may have committed, there is no way to structure appropriate stimuli to detect the telltale knowledge that would result from committing the crime. Brain fingerprinting can, however, be used for specific screening or focused screening, when investigators have some idea what they are looking for. For example, brain fingerprinting can be used to detect whether a person has knowledge that would identify him as an FBI agent, an Al-Qaeda-trained terrorist, a member of a criminal organization or terrorist cell, or a bomb maker (Farwell *et al.* 2006).

Brain fingerprinting does not detect lies. It simply detects information. No questions are asked or answered during a brain fingerprinting test. The subject neither lies nor tells the truth during a brain fingerprinting test, and the outcome of the test is unaffected by whether he has lied or told the truth at any other time. The outcome of "information present" or "information absent" depends on whether the relevant information is stored in the brain, and not on what the subject says about it (Farwell 1994, Simon 2005, PBS 2004).

Brain fingerprinting does not determine whether a suspect is guilty or innocent of a crime. This is a legal determination to be made by a judge and jury, not a scientific determination to be made by a computer or a scientist (Farwell 1994, PBS 2004). Brain fingerprinting can provide scientific evidence that the judge and jury can weigh along with the other evidence in reaching their decisions regarding the crime. To remain within the realm of scientific testimony, however, a brain fingerprinting expert witness must testify only regarding the scientific test and information stored in the brain revealed by the test, as Dr. Farwell did in the Harrington case (Harrington v. State). Like the testimony of other forensic scientists, a brain fingerprinting scientist's testimony does not include interpreting the scientific evidence in terms of guilt or innocence. A DNA expert may testify that two DNA samples match, one from the crime scene and one from the suspect, but he does not conclude "this man is a murderer." Similarly, a brain fingerprinting expert can testify to the outcome of the test that the subject has specific information stored in his brain about the crime (or not), but the interpretation of this evidence in terms of guilt or innocence is solely up to the judge and jury (Harrington v. State, PBS 2004).

Just as all witness testimony depends on the memory of the witness, brain fingerprinting depends on the memory of the subject. Like all witness testimony, brain fingerprinting results must be viewed in light of the limitations on human memory and the factors affecting it (Harrington v. State, PBS 2004). Brain fingerprinting can provide scientific evidence regarding what information is stored in a subject's brain. It does not determine what information *should be*, *could be*, or *would be* stored in the subject's brain if the subject were innocent or guilty. It only measures what actually *is* stored in the brain. How this evidence is interpreted, and what conclusions are drawn based on it, is outside the realm of the science and the scientist. This is up to the judge and jury. It is up to the prosecutor and the defense attorney to argue, and the judge and jury to decide, the significance and weight of the brain fingerprinting evidence in making a determination of whether or not the subject committed the crime.

Like all forensic science techniques, brain fingerprinting depends on the evidence-gathering process which lies outside the realm of science to provide the evidence to be scientifically tested. Before a brain fingerprinting test can be conducted, an investigator must discover relevant information about the crime or investigated situation. This investigative process, in which the investigator gathers the information to be tested from the crime scene or other sources related to the crime, depends on the skill and judgment of the investigator. This process is outside the scientific process; it precedes the scientific process of brain fingerprinting. This investigative process produces the probe stimuli to be tested. Brain fingerprinting science only determines whether the information tested is stored in the brain of the subject or not. It does not provide scientific data on the effectiveness of the investigation that produced the information about the crime that was tested. In this regard, brain fingerprinting is similar to other forensic sciences. A DNA test determines only whether two DNA samples match, it does not determine whether the investigator did an effective job of collecting DNA from the crime scene. Similarly, a brain fingerprinting test determines only whether or not the information stored in the suspect's brain matches the information contained in the probe stimuli. This is information that the investigator provided to the scientist to test scientifically, based on the investigative process that is outside the realm of science. In making their determination about the crime and the suspect's possible role in it, the judge and jury must take into account not only the scientific determination of "information present" or "information absent" provided by the brain fingerprinting test; they must also make common-sense, human, non-scientific judgments regarding the information gathered by the investigator and to what degree knowledge or lack of knowledge of that information sheds light on the suspect's possible role in the crime (Harrington v. State, Farwell1995a). Brain fingerprinting is not a substitute for effective investigation on the part of the investigator or for common sense and good judgment on the part of the judge and jury (PBS 2004).

Future applications and research

After Dr. Farwell invented Brain Fingerprinting, he withheld it from the public for 15 years while he, his colleagues, and other, independent scientists tested it in the laboratory and in the field (Farwell *et al.* 2006, ABC Good Morning America 2004). Farwell's decision to apply this science in real-life situations has been controversial (Dale 2001). In the years since Dr. Farwell first began applying the technology in the real world, proponents, including other scientists who have successfully applied the technique such as FBI scientist Drew Richardson, and those who have been freed or otherwise helped by brain fingerprinting, have advocated continuing and expanded application of the technology in the real world (Farwell *et al.* 2006, ABC Good Morning America 2004, CBS 60 Minutes 2000). Critics, including some scientists, and those whose criminal activities have been thwarted by brain fingerprinting have advocated further delay in applying the technique (Fox 2006b, Abdollah 2003, Rosenfeld 2005, KTVO-TV 1999).

According to sworn testimony by Dr. William Iacono, an independent expert unaffiliated with Dr. Farwell who has conducted extensive research in the area, the science underlying brain fingerprinting has been published in hundreds, perhaps thousands, of

articles in the scientific literature, and the specific application of this science in detecting information has been published in about 50 studies (Harrington v. State). Although the science is well established, opinions among scientists and others on the social policy question of how and when this science should be applied vary widely (Fox 2006b, Abdollah 2003). Dr. Farwell's decision to apply this science in bringing criminals to justice (Dalbey 1999) and freeing innocent suspects (Harrington v. State) is controversial (Fox 2006b, Abdollah 2003, Dale 2001, ABC Good Morning America 2004, CBS 60 Minutes 2000). Various other attempts to apply this science in the detection of concealed information have varied in accuracy and efficacy, depending on the scientific procedures used (Harrington v. State).

Farwell and colleagues (e.g. Farwell & Smith 2001) as well as other, independent scientists who have precisely replicated Farwell's research or used similar methods (e.g., Iacono and colleagues, Allen & Iacono 1997), have obtained accuracy rates approaching 100% in both laboratory and field conditions (Farwell *et al.* 2006, Farwell & Richardson 2006).

Different scientific methods, however, have yielded different results. In P300-based tests using different experimental methods, different brain responses, different stimulus types, different data collection methods, different analysis methods, and different statistics from those used in Farwell's brain fingerprinting, Rosenfeld reported accuracy rates close to those obtained by chance, even without countermeasures (Rosenfeld *et al.* 2004). Moreover, Rosenfeld's alternative technique proved susceptible to countermeasures (Rosenfeld *et al.* 2004).

Controversy has arisen over the best explanation for the fact that Farwell and others who use similar scientific methods have achieved near-100% accuracy (Farwell *et al.* 2006), while Rosenfeld's alternative method yielded variable accuracy, sometimes as low as chance (Rosenfeld *et al.* 2004).

Farwell, FBI scientists Drew Richardson and Sharon Smith, and other brain fingerprinting experts claim that one cannot necessarily expect to obtain the same accuracy as brain fingerprinting without following standard brain fingerprinting scientific protocols or similar methods, that Rosenfeld's failure to achieve accuracy rates comparable to those of brain fingerprinting is the result of the substantial differences in scientific methodology between his alternative technique and brain fingerprinting, and therefore the fact that Rosenfeld's alternative technique is admittedly inaccurate and susceptible to countermeasures (Rosenfeld *et al.* 2004) is no reflection on brain fingerprinting (Farwell & Smith 2001, Farwell & Richardson 2006, Farwell *et al.* 2006, Simon 2005).

Proponents advocate continuing the use of brain fingerprinting to bring criminals and terrorists to justice and to free innocent suspects, while at the same time more research is continuing. Dr. Farwell and former FBI scientist Dr. Drew Richardson are among the scientists who advocate continuing the use of brain fingerprinting in criminal

investigations and counterterrorism, without delay, as well as ongoing research on the technology (Farwell & Richardson 2006, Simon 2005).

Dr. Farwell was interviewed by *TIME* magazine after he was selected to the TIME 100: The Next Wave, the 100 innovators who may be "the Picassos or Einsteins of the 21st Century." He said, "The fundamental task in law enforcement and espionage and counterespionage is to determine the truth. My philosophy is that there is a tremendous cost in failing to apply the technology." (Dale 2001)

Critics of brain fingerprinting claim that the inaccuracy and susceptibility to countermeasures of Rosenfeld's alternative technique also cast doubt on all P300-based information-detection techniques, including brain fingerprinting (Rosenfeld 2005). Critics agree with proponents that ongoing research on brain fingerprinting is valuable and desirable (Fox 2006b, Abdollah 2003). Unlike proponents, however, critics advocate a discontinuation of the use of brain fingerprinting in criminal and counterterrorism cases while this research is continuing (Fox 2006b, Abdollah 2003).

A report by the United States General Accounting Office (now called Government Accountability Office) in 2001 reported that the scientists it interviewed (including Farwell, Iacono, Richardson, Rosenfeld, Smith, Donchin, and others) all had expressed a need for more research to investigate brain fingerprinting's application as forensic science tool (Initial GAO Report). While they were unanimous in their support of more scientific research, scientists and others expressed widely varying views on the social policy question of whether brain fingerprinting should continue to be applied to bring criminals and terrorists to justice and to free innocent suspects while this research continues. The initial GAO report was completed before the terrorist attacks of 9/11/2001, when the primary interest of federal agencies in detection methods was for employee screening, rather than detecting terrorists. (As discussed above, brain fingerprinting is not applicable in general employee screening.) Senator Charles Grassley, who commissioned the initial report, has asked the GAO produce a new report that examines the value of brain fingerprinting in counterterrorism and criminal investigations in the post-911 world in light of published scientific research on the application of the technique in the laboratory and the field (Fox 2006a).

Proponents of the continued use of brain fingerprinting in criminal and counterterrorism cases cite the peer-reviewed research on the accuracy of brain fingerprinting in the laboratory and the field, the fact that it has been ruled admissible in court, the vital counterterrorism applications, and the benefits of bringing criminals such as serial killer JB Grinder to justice and freeing innocent convicts such as Terry Harrington. They emphasize the established science, the proven accuracy of brain fingerprinting when practiced according to standard brain fingerprinting scientific protocols, and the fact that brain fingerprinting is voluntary and non-invasive. They advocate continuing to use brain fingerprinting in criminal investigations and counterterrorism while research on the technique continues (ABC Good Morning America 2004 ABC-TV Good Morning America: Charles Gibson interviews Dr. Lawrence Farwell, CBS 60 Minutes: Mike

Wallace interviews Dr. Lawrence Farwell, Simon 2005 “What you don’t know can’t hurt you,” *Law Enforcement Technology*.

Critics cite the inaccuracy and susceptibility to countermeasures of Rosenfeld’s alternative technique, and suggest that this casts doubt on brain fingerprinting as well (Rosenfeld 2005). They emphasize the uncertainty of applying new technology while it is still being researched, and advocate discontinuing the use of brain fingerprinting in criminal and counterterrorism cases until more research has been completed (Fox 2006b "Brain Fingerprinting Skepticism", Abdollah 2003 "Issues: Brain Fingerprinting").

Those personally affected by brain fingerprinting have expressed divergent views as well, particularly on the issue of delaying the application of brain fingerprinting in criminal cases. Terry Harrington, for whom brain fingerprinting provided exculpatory evidence that was ruled admissible in court (Harrington v. State, Farwell & Makeig 2005), and who was subsequently released from prison after serving 24 years for a murder he did not commit, has advocated continuing to apply brain fingerprinting in criminal cases while the research continues (CBS 60 Minutes 2000).

JB Grinder, whose 15-year string of serial rapes and murders was cut short after Farwell’s brain fingerprinting test detected the record of the murder of Julie Helton stored in his brain, would have strongly preferred that applications of the technique in criminal investigations be delayed indefinitely (KTVO-TV 1999).

In the case of Jimmy Ray Slaughter, an Oklahoma court ruled that exculpatory evidence from a brain fingerprinting test conducted by Dr. Farwell was “untimely” and had been obtained too late to be used in his appeals (Slaughter v. State). Despite the “untimely” exculpatory evidence – which also included exculpatory DNA evidence, an FBI report discrediting key forensic evidence that had been used against him at trial, and the sworn testimony of the original chief investigator on his case, who became convinced that Slaughter was innocent – Slaughter was executed (Slaughter v. State). Until his execution, Slaughter strongly opposed any delay in applying brain fingerprinting in criminal cases on the grounds that any delay would cost more innocent lives, both of murder victims and of falsely convicted people – as he claimed to be himself – who could be saved by brain fingerprinting only if it was applied soon enough (ABC Good Morning America 2004).

Before Slaughter was executed, when it appeared that brain fingerprinting and other exculpatory evidence may have arrived in time to overturn his conviction, Farwell said, "When Jimmy Ray Slaughter came to me for help, he had a life expectancy of about 90 days. I had to say yes or no. I couldn't say 'wait'. I said yes, and I believe this was the right decision for me. If my already well-proven invention can save innocent lives while still more research is going on, I believe it is my responsibility as a scientist to make it available." (Witchalls 2004)

Dr. Farwell told Mike Wallace in an interview on CBS 60 Minutes, “Brain Fingerprinting is a scientific technique for determining whether certain information is stored in the brain

or not by measuring brain waves, electrical brain activity. The fundamental difference between an innocent person and a guilty person is that a guilty person, having committed the crime, has the record stored in his brain. Now we have a way to measure that scientifically." (CBS 60 Minutes 2000)

In an interview with Charles Gibson on Good Morning America, Dr. Farwell stated, "We showed not only in the laboratory but in over 100 actual real-life situations that the technology was effective. And to date we have never gotten a wrong answer." (ABC Good Morning America 2004) ABC-TV Good Morning America: Charles Gibson interviews Dr. Lawrence Farwell

Chapter- 7

Telephone Tapping

Telephone tapping (also **wire tapping** or **wiretapping** in American English) is the monitoring of telephone and Internet conversations by a third party, often by covert means. The wire tap received its name because, historically, the monitoring connection was an actual electrical tap on the telephone line. Legal wiretapping by a government agency is also called lawful interception. *Passive wiretapping* monitors or records the traffic, while *active wiretapping* alters or otherwise affects it.

Legal status

Telephone line control device "Jitka", used in late 1960s by Czech StB to signal line occupancy, and connect a recorder

Telephone tapping is officially strictly controlled in many countries to safeguard a person's privacy; this is the case in all developed democracies. In theory, telephone tapping often needs to be authorized by a court, and is, again in theory, normally only approved when evidence shows it is not possible to detect criminal or subversive activity in less intrusive ways; often the law and regulations require that the crime investigated must be at least of a certain severity. In many jurisdictions however, permission for telephone tapping is easily obtained on a routine basis without further investigation by the court or other entity granting such permission. Illegal or unauthorized telephone tapping is often a criminal offense. However, in certain jurisdictions such as Germany, courts will accept illegally recorded phone calls without the other party's consent as evidence, but the unauthorized telephone tapping will be avenged too.

In the United States, federal agencies may be authorized to engage in wiretaps by the United States Foreign Intelligence Surveillance Court, a court with secret proceedings, in certain circumstances.

Under United States federal law and most state laws, there is nothing illegal about one of the parties to a telephone call recording the conversation, or giving permission for calls to be recorded or permitting their telephone line to be tapped. However the telephone recording laws in most U.S. states require only one party to be aware of the recording, while 12 states require both parties to be aware. It is considered better practice to announce at the beginning of a call that the conversation is being recorded.

Methods

Official use

The contracts or licenses by which the state controls telephone companies often require that the companies must provide access for tapping lines to law enforcement. In the U.S., telecommunications carriers are required by law to cooperate in the interception of communications for law enforcement purposes under the terms of Communications Assistance for Law Enforcement Act (CALEA).

When telephone exchanges were mechanical, a tap had to be installed by technicians, linking circuits together to route the audio signal from the call. Now that many exchanges have been converted to digital technology tapping is far simpler and can be ordered remotely by computer. Telephone services provided by cable TV companies also use digital switching technology. If the tap is implemented at a digital switch, the switching computer simply copies the digitized bits that represent the phone conversation to a second line and it is impossible to tell whether a line is being tapped. A well-designed tap installed on a phone wire can be difficult to detect. In some instances some law enforcement maybe able to even access a mobile phone's internal microphone even while it isn't actively being used on a phone call (unless the battery is removed). The noises that some people believe to be telephone taps are simply crosstalk created by the coupling of signals from other phone lines.

Data on the calling and called number, time of call and duration, will generally be collected automatically on all calls and stored for later use by the billing department of the phone company. These data can be accessed by security services, often with fewer legal restrictions than for a tap. This information used to be collected using special equipment known as *pen registers* and *trap and trace devices* and U.S. law still refers to it under those names. Today, a list of all calls to a specific number can be obtained by sorting billing records. A telephone tap during which only the call information is recorded but not the contents of the phone calls themselves, is called a *pen register* tap.

For telephone services via digital exchanges, the information collected may additionally include a log of the type of communications media being used (some services treat data and voice communications differently to conserve bandwidth).

Non-official use

A telephone recording adapter (in-line tap). The phone jack connects to the wall socket while the phone being monitored is connected to the adapter's socket. The audio plug connects to the recording device (computer, tape recorder, etc).

Conversations can be recorded or monitored unofficially, either by tapping by a third party without the knowledge of the parties to the conversation, or recorded by one of the parties. This may or may not be illegal, according to the circumstances and the jurisdiction.

There are a number of ways to monitor telephone conversations. One of the parties may record the conversation by several methods, either on a tape or solid-state recording device, or on a computer running call recording software. The recording,whether overt or covert, may be started manually, automatically by detecting sound on the line (VOX), or automatically whenever the phone is off the hook.

- using an inductive coil tap (telephone pickup coil) attached to the handset or near the base of the telephone;
- fitting an in-line tap, as discussed below, with a recording output;
- using an in-ear microphone while holding the telephone to the ear normally; this picks up both ends of the conversation without too much disparity between the volumes
- more crudely and with lower quality, simply using a speaker-phone and recording with a normal microphone

The conversation may be monitored (listened to or recorded) covertly by a third party by using an induction coil or a direct electrical connection to the line using a beige box. An induction coil is usually placed underneath the base of a telephone or on the back of a telephone handset to pick up the signal inductively. An electrical connection can be made anywhere in the telephone system, and need not be in the same premises as the telephone. Some apparatus may require occasional access to replace batteries or tapes. Poorly designed tapping or transmitting equipment can cause interference audible to users of the telephone.

The tapped signal may either be recorded at the site of the tap or transmitted by radio or over the telephone wires. As of 2007 state-of-the-art equipment operates in the 30–300 GHz range. The transmitter may be powered from the line to be maintenance-free, and only transmits when a call is in progress. These devices are low-powered as not much power can be drawn from the line, but a state-of-the-art receiver could be located as far away as ten kilometers under ideal conditions, though usually located much closer. Research has shown that a satellite can be used to receive terrestrial transmissions with a power of a few milliwatts. Any sort of radio transmitter whose presence is suspected is detectable with suitable equipment.

Conversation on many early cordless telephones could be picked up with a simple radio scanner or sometimes even a domestic radio. Widespread digital spread spectrum technology and encryption make eavesdropping this way much more difficult.

A problem with recording a telephone conversation is that the recorded volume of the two speakers may be very different. A simple tap will have this problem. An in-ear microphone, while involving an additional distorting step by converting the electrical signal to sound and back again, in practice gives better-matched volume. Dedicated, and relatively expensive, telephone recording equipment equalises the sound at both ends from a direct tap much better.

Location data

Mobile phones are, in surveillance terms, a major liability. This liability will only increase as the new third-generation (3G) phones are introduced, as the base stations will be located closer together. For mobile phones the major threat is the collection of communications data. This data does not only include information about the time, duration, originator and recipient of the call, but also the identification of the base station where the call was made from, which equals its approximate geographical location. This data is stored with the details of the call and has utmost importance for traffic analysis.

It is also possible to get greater resolution of a phone's location by combining information from a number of cells surrounding the location, which cells routinely communicate (to agree on the next handoff—for a moving phone) and measuring the timing advance, a correction for the speed of light in the GSM standard. This additional precision must be specifically enabled by the telephone company - it is not part of ordinary operation.

The second generation mobile phones (circa 1978 through 1990) could be easily monitored by anyone with a 'scanning all-band receiver' because the system used an analog transmission system-like an ordinary radio transmitter. The third generation digital phones are harder to monitor because they use digitally-encoded and compressed transmission. However the government can tap mobile phones with the cooperation of the phone company. It is also possible for organizations with the correct technical equipment to monitor mobile phone communications and decrypt the audio. A device called an "IMSI-catcher" pretends to the mobile phones in its vicinity to be a legitimate base station of the mobile phone network, subjecting the communication between the phone and the network to a man-in-the-middle attack. This is possible because while the mobile phone has to authenticate itself to the mobile telephone network, the network does not authenticate itself to the phone. Once the mobile phone has accepted the IMSI-catcher as its base station the IMSI-catcher can deactivate GSM encryption using a special flag. All calls made from the tapped mobile phone go through the IMSI-catcher and are then passed on to the mobile network. Some phones include a special monitor mode (activated with secret codes or special software) which displays GSM operating parameters such as encryption while a call is being made. There is no defense against IMSI-catcher based eavesdropping, except using end-to-end call encryption; products offering this feature, secure telephones, are already beginning to appear on the market, though they tend to be expensive and incompatible with each other, which limits their proliferation.

Internet

In 1995, Peter Garza, a Special Agent with the Naval Criminal Investigative Service, conducted the first court-ordered Internet wiretap in the United States while investigating Julio Cesar Ardita ("El Griton").

As technologies emerge, including VoIP, new questions are raised about law enforcement access to communications. In 2004, the Federal Communications Commission was asked to clarify how the Communications Assistance for Law Enforcement Act (CALEA)

related to Internet service providers. The FCC stated that “providers of broadband Internet access and voice over Internet protocol (“VoIP”) services are regulable as “telecommunications carriers” under the Act.” Those affected by the Act will have to provide access to law enforcement officers who need to monitor or intercept communications transmitted through their networks. As of 2009, warrantless surveillance of internet activity has consistently been upheld in FISA court.

The Internet Engineering Task Force has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.

Typically, illegal Internet wiretapping will be conducted via Wi-Fi connection to someone's internet by cracking the WEP or WPA key, using a tool such as Aircrack-ng or Kismet. Once in, the intruder will rely on a number of potential tactics, for example an ARP spoofing attack which will allow the intruder to view packets in a tool such as Wireshark or Ettercap.

One issue that Internet wiretapping is yet to overcome is that of steganography, whereby a user encodes, or “hides”, one file inside another (usually a larger, dense file like a MP3 or JPEG image). With modern advancements in encoding technologies, the resulting combined file is essentially indistinguishable to anyone attempting to view it, unless they have the necessary protocol to extract the hidden file. US News reported that this technique was commonly used by Osama bin Laden as a way to communicate with his terrorist cells.

There are a number of steganographic programs available online, such as Wnstorm, QuickCrypto, and TextHide.

Webtapping

Though the practice is more closely analogous to call tracing, logging the IP addresses of users that access certain websites is commonly called "Webtapping".

Webtapping is used to monitor websites that presumably contain dangerous or sensitive materials, and the people that access them. Though it is allowed by the USA PATRIOT Act, it is considered by many a questionable practice, if not an all-out violation of civil liberties.

History

Telephone wiretapping began in the 1890s, following the invention of the telephone recorder, and its constitutionality was established in the Prohibition Era conviction of bootlegger Roy Olmstead. Wiretapping has also been carried out under most Presidents, sometimes with a lawful warrant since the Supreme Court ruled it constitutional in 1928. On October 19, 1963, U.S. Attorney General Robert F. Kennedy, who served under John F. Kennedy and Lyndon B. Johnson, authorized the FBI to begin wiretapping the

communications of Rev. Martin Luther King, Jr. The wiretaps remained in place until April 1965 at his home and June 1966 at his office.

The history of voice communication technology begins in 1876 with the invention of Alexander Graham Bell's telephone. In the 1890s, "law enforcement agencies begin tapping wires on early telephone networks". Remote voice communications "were carried almost exclusively by circuit-switched systems," where telephone switches would connect wires to form a continuous circuit and disconnect the wires when the call ended). All other telephone services, such as call forwarding and message taking, were handled by human operators. However, the first computerized telephone switch was developed by Bell Labs in 1965. This got rid of standard wiretapping techniques.

In the 1970s, optical fibers become a medium for telecommunications. These fiber lines, which are "long, thin strands of glass that carry signals via laser light," are more secure than radio, and have become very cheap. From the 1990s to the present, the majority of communications from "one fixed location to another have moved by fiber." Since these fiber communications are "wired," U.S. law "gives them greater protection."

The earliest wiretaps were extra wires—"connected to the line between the telephone company's central office and the subscriber—that carried the signal to a pair of earphones and a recorder. Later on, wiretaps were installed at the central office on the frames that held the incoming wires".

Before the Japanese attack on Pearl Harbor and the subsequent entry of the United States into World War II, the U.S. House of Representatives held hearings on the legality of wiretapping for national defense. Significant legislation and judicial decisions on the legality and constitutionality of wiretapping had taken place years before World War II. However, it took on new urgency at that time of national crisis. The actions of the government regarding wiretapping for the purpose of national defense in the current war on terror have drawn considerable attention and criticism. In the World War II era, the public was also aware of the controversy over the question of the constitutionality and legality of wiretapping. Furthermore, the public was concerned with the decisions that the legislative and judicial branches of the government were making regarding wiretapping.

In the Greek telephone tapping case 2004-2005 more than 100 mobile phone numbers belonging mostly to members of the Greek government, including the Prime Minister of Greece, and top-ranking civil servants were found to have been illegally tapped for a period of at least one year. The Greek government concluded this had been done by a foreign intelligence agency, for security reasons related to the 2004 Olympic Games, by unlawfully activating the lawful interception subsystem of the Vodafone Greece mobile network. An Italian tapping case which surfaced in November 2007 revealed significant manipulation of the news at the national television company RAI.

CrimethInc. sticker on a telephone warning users of phone tapping by the U.S. government

In 1967, the U.S. Supreme Court ruled that wiretapping (or "intercepting communications") requires a warrant in the Katz v. United States case. In 1968, Congress passed a law that provided warrants for wiretapping in criminal investigations. In 1978, the Foreign Intelligence Surveillance Act (FISA) created a "secret federal court for issuing wiretap warrants in national security cases." This was in response to findings from the Watergate break-in, which allegedly uncovered a history of presidential operations that had used surveillance on domestic and foreign political organizations.

In 1994, Congress approved the Communications Assistance for Law Enforcement Act (CALEA), which "requires telephone companies to be able to install more effective wiretaps. In 2004, the Federal Bureau of Investigation (FBI), United States Department of Justice (DOJ), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and Drug Enforcement Agency (DEA) wanted to expand CALEA requirements to VoIP service."

The Federal Communications Commission (FCC) ruled in August 2005 that “broadband-service providers and interconnected VoIP providers fall within CALEA’s scope. Currently, instant messaging, web boards and site visits are not included in CALEA’s jurisdiction. In 2007, Congress amended FISA to “allow the government to monitor more communications without a warrant.” In 2008, President George W. Bush expanded the surveillance of internet traffic to and from the U.S. government by signing a national security directive.

In 2008, Wired and other media reported a lamplighter disclosed a "Quantico Circuit" — a 45 megabit/second DS-3 line linking a carrier's most sensitive network in an affidavit that was the basis for a lawsuit against Verizon Wireless. The circuit provides direct access to all content and all information concerning the origin and termination of telephone calls placed on the Verizon Wireless network as well as the actual content of calls, according to the filing.

The most recent case of U.S. wiretapping was the NSA warrantless surveillance controversy discovered in December 2005. It aroused much controversy, after then President George W. Bush admitted to violating a specific federal statute (FISA) and the warrant requirement of the Fourth Amendment to the United States Constitution. The President claimed his authorization was consistent with other federal statutes (AUMF) and other provisions of the Constitution, was necessary to keep America safe from terrorism, and could lead to the capture of notorious terrorists responsible for the September 11 attacks in 2001.

One difference between foreign wiretapping and domestic wiretapping is that, when operating in other countries, “American intelligence services could not place wiretaps on phone lines as easily as they could in the U.S.” Also, domestically, wiretapping is regarded as an extreme investigative technique, whereas outside of the country, the interception of communications is huge. The National Security Agency (NSA) “spends billions of dollars every year intercepting foreign communications from ground bases, ships, airplanes and satellites”.

FISA distinguishes between U.S. persons and foreigners, between communications inside and outside the U.S., and between wired and wireless communications. Wired communications within the U.S. are protected, since intercepting them requires a warrant.

NSA warrantless surveillance controversy

In the most recent issue concerning warrantless wiretapping, earlier in 2007 a Foreign Intelligence Surveillance Act (FISA) court ruled that it increased restraints on the National Security Agency (NSA). The new court ruling requires the NSA to obtain a warrant when intercepting or eavesdropping on foreign-to-foreign intelligence if it passes through any U.S. networks. The Bush Administration in response to this passed a stopgap legislation very quickly through congress that only temporarily relieves the NSA of this prior ruling. Director of National Intelligence Mike McConnell said to Congress that the new ruling could potentially decrease the amount of useful information they collected on

groups like al Qaeda by almost two thirds. He also stated that applying for a warrant can run up to 90 pages and can be time consuming and labor intensive.

Very active in this issue is The American Civil Liberties Union (ACLU). The ACLU has brought about many legal cases challenging the constitutionality of the bill, asserting that it violates Americans' right to free speech and privacy. They have filed lawsuits, motions, and complaints in over 27 states so far to oppose any legislation that encourages unchecked government surveillance. In response to the government arguments, Caroline Fredrickson, Director of the ACLU Washington Legislative Office has said of the bill: "Where will Congress go from here? More unfettered power for an administration that has no respect for the privacy of the citizenry that elected it?"

The stopgap that was hastily put in place by the former Bush Administration expired in February 2008. By then, Congress and FISA reached a compromise on the details of the bill. ACLU advocates pushed to require NSA to provide individual warrants when Americans are involved and on the other hand, U.S. intelligence agencies and the Administration wanted as few obstacles in their way of intercepting private information. Both sides have both shown the possibility for a compromise to accept a Bill that would require a FISA court to approve NSA's procedures while intercepting foreign intelligence when it involves Americans.

However, a later addition to this bill, that was insisted on by then President Bush and Mike McConnell, granted retroactive immunity to telecommunications companies for any "intelligence activity involving communications" that was "designed to detect or prevent a terrorist attack" or attack preparations. The Bush Administration has acknowledged that intelligence agencies conducted warrantless eavesdropping on Americans with the help of Telecom companies such as Verizon, AT&T, and Qwest. All three of these Telecom companies faced multiple civil lawsuits related to their handling of phone records and the passing of this bill granted them immunity.

In favor of the bill, McConnell has said, such immunity was necessary to prevent the telecoms from being bankrupted and to encourage them to continue to cooperate with intelligence agencies. Bush said that he would veto any intelligence bill passed that did not include immunity. Liz Rose, spokeswoman for the Washington office of the ACLU, says the language of the bill is a "blank check" that would cover not only the warrantless wiretapping program the Bush administration has acknowledged, but any unconfirmed or previously unknown program. Sen. Russ Feingold, D-Wis., promised to lead a filibuster to block approval of retroactive immunity. "Retroactive immunity set the terrible precedent that breaking the law is permissible and companies need not worry about the privacy of their customers," Feingold said.

Chapter- 8

Offender Profiling

Offender profiling, also known as **criminal profiling**, is a behavioral and investigative tool that is intended to help investigators to profile unknown criminal subjects or offenders. Offender profiling is also known as criminal profiling, criminal personality profiling, criminological profiling, behavioral profiling or criminal investigative analysis. Geographic profiling is another method to profile an offender. Television shows such as *Law & Order: Criminal Intent*, *Profiler* in the 1990s, the 2005 television series *Criminal Minds*, and the 1991 film *The Silence of the Lambs* have lent many names to what the FBI calls "criminal investigative analysis."

Holmes and Holmes (2008) outline the three main goals of criminal profiling:

- The first is to provide law enforcement with a social and psychological assessment of the offender;
- The second goal is to provide law enforcement with a “psychological evaluation of belongings found in the possession of the offender” (p. 10);
- The third goal is to give suggestions and strategies for the interviewing process.

In modern criminology, offender profiling is generally considered the "third wave" of investigative science:

- the first wave was the study of clues, pioneered by Scotland Yard in the 19th century;
- the second wave was the study of crime itself (frequency studies and the like);
- this third wave is the study of the psyche of the criminal.

There is little empirical evidence that profiling is effective. It mostly rests on 'common sense' justifications. In a controlled situation, professional profilers were no better than laymen in predicting criminals' cognitive processes, physical attributes, offense behaviors, or social habits and history. Overall, the predictive abilities of both laymen and professional profilers was low.

Definitions

Offender profiling is a method of identifying the perpetrator of a crime based on an analysis of the nature of the offense and the manner in which it was committed. Various aspects of the criminal's personality makeup are determined from his or her choices before, during, and after the crime. This information is combined with other relevant details and physical evidence, and then compared with the characteristics of known personality types and mental abnormalities to develop a practical working description of the offender.

Psychological profiling may be described as a method of suspect identification which seeks to identify a person's mental, emotional, and personality characteristics (as manifested in things done or left at the crime scene). This was used in the investigation of the serial murders committed by Ted Bundy. Dr. Richard B. Jarvis, a psychiatrist with expertise on the criminal mind, predicted the age range of Bundy, his sexual psychopathy, and his above average intellect.

Another good example and more depth of how psychological profiling could be done is on the investigation on Gary Leon Ridgway, also known as the Green River Killer. An investigator named John E. Douglas who worked for the FBI provided a twelve-page profile. Briefly, it stated these points:

- Probably a white male who had a dysfunctional relationship with women.
- Organized since he tried to hide the bodies and appeared to spend some time at the river
- Cunning in using rocks to weigh the victims down in the water to conceal them.
- Very mobile with a vehicle.
- Going to kill again.
- Like other serial killers, he would be prone to contacting police wanting to help in the investigations.

History

The origins of profiling can be traced back to as early as the Middle Ages, with the inquisitors trying to “profile” heretics. Jacob Fries, Cesare Lombroso, Alphonse Bertillon, Hans Gross and several others realized the potential of profiling in the 19th century although their research is generally considered to be prejudiced, reflecting the biases of their time.

Notable profilers

Thomas Bond

During the 1880s, Thomas Bond, a medical doctor, tried to profile the personality of Jack the Ripper. Bond, a police surgeon, assisted in the autopsy on Mary Kelly. In his notes, dated November 10, 1888, he mentioned the sexual nature of the murders coupled with

elements of apparent misogyny and rage. Dr. Bond also tried to reconstruct the murder and interpret the behavior pattern of the offender: soon he came up with a profile or signature personality traits of the offender to assist police investigation. The profile said that five murders of seven in the area at the time the report was written had been committed by one person alone who was physically strong, composed, and daring. The unknown offender would be quiet and harmless in appearance, possibly middle-aged, and neatly attired, probably wearing a cloak to hide the bloody effects of his attacks out in the open. He would be a loner, without a real occupation, eccentric, and mentally unstable. He might even suffer from a condition called Satyriasis, a sexual deviancy that is today referred to as hypersexuality or promiscuity. Bond also mentioned that he believed the offender had no anatomical knowledge and could not be a surgeon or butcher. Moreover, Dr. Bond later concluded that the same offender was responsible for the murder of Alice McKenzie.

Walter C. Langer

In 1943, William J. Donovan, chief of the US Office of Strategic Services (OSS), asked Dr. Walter C. Langer, a psychoanalyst based in Boston, to develop a “profile” of Adolf Hitler. What the OSS wanted was a behavioral and psychological analysis for the construction of strategic plans, given various options.

Dr. Langer used speeches, Hitler's book Mein Kampf, interviews with people who had known Hitler and some four hundred published works to complete his wartime report, which was eventually declassified by OSS and published by Langer (along with certain collateral material) as The Mind of Adolf Hitler in 1972. This work contains a profile of possible behavioural traits of Hitler, and his possible reactions to the idea of Germany losing World War II. Dr. Langer’s profile noted that Hitler was meticulous, conventional, and prudish about his appearance and body. He was robust and viewed himself as a standard-bearer and trendsetter. He had manic phases, yet took little exercise. Due to a lack of evidence, Langer believed that Hitler was in reasonably good health, so it was unlikely he would die from natural causes, but he was deteriorating mentally. He would not try to escape to a neutral country, nor would he (in Langer's opinion) allow himself to be captured by the Allies. Hitler always walked diagonally from one corner to another when crossing a room, and he whistled a marching tune. He feared syphilis and germs.

Langer's profile also pointed out Hitler's oedipal complex, with the effect being the need to prove his manhood to his mother, and his masochistic coprolagnia and urolagnia. He detested the learned and the privileged, but enjoyed classical music, vaudeville, and Richard Wagner's opera. He showed strong streaks of sadism and liked circus acts that were risky and dangerous. He tended to speak in long monologues rather than have conversations. He had difficulty establishing close relationships with anyone. Since he appeared to be delusional, it was possible that his psychological structures would collapse in the face of imminent defeat. The most likely scenario was that he would commit suicide, although there was a possibility that he would order a henchman to perform euthanasia.

James A. Brussel

Between 1940 and 1956, a serial bomber terrorized New York City by planting bombs in public places including movie theaters, phone booths, Radio City Music Hall, Grand Central Terminal, and Pennsylvania Station. In 1956, the frustrated police requested a profile from Greenwich Village psychiatrist James A. Brussel, who was New York State's assistant commissioner of mental hygiene. Dr. Brussel studied photographs of the crime scenes and analyzed the so called “mad bomber’s” mails to the press. Soon he came up with a detailed description of the offender. In his profile, Dr. Brussel suggested that the unknown offender would be a heavy middle-aged man who was unmarried, but perhaps living with a sibling. Moreover, the offender would be a skilled mechanic from Connecticut, who was a Roman Catholic immigrant and, while having an obsessional love for his mother, would harbour a hatred for his father. Brussel noted that the offender had a personal vendetta against Consolidated Edison, the city’s power company; the first bomb targeted its 67th Street headquarters. Dr. Brussel also mentioned to the police that, upon the offender's discovery, the “chances are he will be wearing a double-breasted suit. Buttoned.”

From his profile, it was obvious to the police that the mysterious bomber would be a disgruntled current or unhappy former employee of Con Ed. The profile helped police to track down George Metesky in Waterbury, Connecticut; he had worked for Con Ed in the 1930s. He was arrested in January 1957 and confessed immediately. The police found Brussel’s profile most accurate when they met the heavy, single, Catholic, and foreign-born Metesky. When the police told him to get dressed, he went to his bedroom and returned wearing a double-breasted suit, fully buttoned, just as Dr. Brussel had predicted. However, Malcolm Gladwell has written that offender profiling is not a science at all, but is couched in such ambiguous language that it can support almost any interpretation; and about Brussel says:

Brussel did not really understand the mind of the Mad Bomber. He seems to have understood only that, if you make a great number of predictions, the ones that were wrong will soon be forgotten, and the ones that turn out to be true will make you famous. The Hedunit is not a triumph of forensic analysis. It’s a party trick.

Dr. Brussel assisted New York City police from 1957 to 1972 and profiled many crimes, including murder. Dr. Brussel also worked with other investigative agencies. Brussel’s profile led the Boston Police to the apprehension of Albert DeSalvo, the notorious serial sex murderer known as the Boston Strangler. The media dubbed Dr. Brussel as “Sherlock Holmes of the Couch”.

Howard Teten

Howard D. Teten, a veteran police officer from California, joined the FBI in 1962. He was appointed as an instructor in applied criminology at the old National Police Academy in Washington, D.C. Teten was greatly interested in the application of offender profiling, and had included some of the ideas in his applied criminology course. He met Dr. Brussel

and exchanged investigative ideas and psychological strategies in profiling crimes. Although Teten disagreed with Dr. Brussel's Freudian interpretations, he accepted other tenets of his investigative analysis.

In 1972 the FBI's Behavioral Science Unit at Quantico was formed, with Teten joining FBI Instructor Patrick J. Mullany's team. Teten and Mullany designed a method for analyzing unknown offenders in unsolved cases. The idea was to look at the behavioral manifestations at a crime scene for evidence of mental disorders and other personality traits, thus aiding the detectives' deductive reasoning. Their ideas on offender profiling were tested when a seven-year-old girl was abducted from a Rocky Mountains campsite in Montana in June 1973. The girl was abducted from a tent in the early hours; the offender overpowered her before she could alert her parents, who were sleeping nearby. When an intensive search for the missing child failed, the case was referred to the FBI.

Teten, Mullany and Col. Robert K. Ressler employed their criminal investigative analysis technique to track down the unknown offender. Their profile declared that the abductor was most likely a young, white, male, homicidal Peeping Tom; a sex killer who mutilates his victim after death, who sometimes takes body parts as souvenirs. Later, the profile led to the arrest of David Meirhofer, a local 23-year-old single man who was also a suspect in another murder case. The search of his house unearthed "souvenirs"—body parts taken from both victims. Meirhofer was the first serial killer to be caught with the aid of the FBI's new investigative technique, called offender profiling or criminal investigative analysis. A decade later, the technique became a more sophisticated and systematic profiling tool known as the Criminal Investigative Analysis Program (CIAP).

Richard Walter and Bob Keppel

In 1974, homicide detective Robert D. Keppel used new methods of psychological profiling to investigate notorious serial killers Ted Bundy and the Green River Killer. He combined his field expertise with criminal psychologist Richard Walter. As a psychologist in Michigan's notorious prison system, Walter had interviewed over two thousand murderers, sex-offenders and serial killers. Walter began to see common threads among offenders and was able to group all killings and sex crimes into four distinct "subtypes": power-assertive, power-reassurance, anger-retaliatory, and anger-excitation or sadism. He was the first to develop a matrix using suspect pre-crime, crime and post-crime behaviors as a tool for investigation. Walter later co-founded the Vidocq society, an exclusive organization of forensic professionals who solve cold cases for law enforcement agencies, worldwide. Together, Keppel and Walter created the HITS database, which lists characteristics of violent crimes so that common threads can be investigated. They also published a leading scholarly article for the FBI and violent crime investigators all over the world: "Profiling Killers: A Revised Classification Model for Understanding Sexual Murder".

John Douglas and Robert Ressler

In 1978, after Howard Teten left the Behavioral Science Unit, John Douglas and Robert Ressler became pillars of offender profiling in the FBI. They spent much time studying convicted sex murderers and interviewing them, creating organized and disorganized typology, which is still in use today. Ressler was also responsible for the founding of the National Center for Analysis of Violent Crime (NCAVC) and at least partially responsible for the establishment of VICAP. Their studies provide more information on the behavioral patterns, traits and characteristics of criminals which can then be added to the offender profiling program.

David Canter

In 1986, police forces across the south of England were struggling to find the *Railway Rapist* who was then renamed the *Railway Killer* after murdering a victim for the first time. Dr. David Canter, a psychologist and criminologist then from Surrey University, was invited to compose British crime's first offender profile. When John Duffy was later arrested, charged and convicted, it turned out 13 of Canter's 17 proclamations about the perpetrator were accurate. Profiling became commonplace in large-scale police searches afterwards.

Phases of profiling

According to Gregg O. McCrary, the basic premise is that behavior reflects personality. In a homicide case, for example, FBI profilers try to collect the personality of the offender through questions about his or her behavior at four phases:

1. **Antecedent:** What fantasy or plan, or both, did the murderer have in place before the act? What triggered the murderer to act some days and not others?
2. **Method and manner:** What type of victim or victims did the murderer select? What was the method and manner of murder: shooting, stabbing, strangulation or something else?
3. **Body disposal:** Did the murder and body disposal take place all at one scene, or multiple scenes?
4. **Post-offense behavior:** Is the murderer trying to inject himself into the investigation by reacting to media reports or contacting investigators?

A sexual crime is analyzed in much the same way (bearing in mind that homicide is sometimes a sexual crime), with the additional information that comes from a living victim. Professor David Canter is the pioneer of scientific offender profiling, developing the discipline of Investigative Psychology as a response to his dissatisfaction with the scientific bases for this activity. The IAIP of which Canter is President now seeks to set professional guidelines for practice and research in this area.

Another phase of criminal profiling (crime scene investigation) is case linkage. According to Brent E. Turvey, case linkage or linking analysis refers to the process of

determining whether or not there are discrete connections between two or more previously unrelated cases through crime scene analysis. It involves establishing and comparing the physical evidence, victimology, crime scene characteristics, modus operandi (MO), and signature behaviors between each of the cases under review. It has two purposes:

1. To assist law enforcement with the application of its finite resources by helping to establish where to apply investigative efforts and
2. To assist the court in determining whether or not there is sufficient behavioral evidence to suggest a common scheme or plan in order to address forensic issues, such as whether similar crimes may be tried together or whether other crimes may be brought in as evidence.

With respect to behavioral evidence, case linkage efforts have most typically hinged on two concepts:

1. MO, modus operandi
2. Signature

Controversies

Although offender profiling has earned much public attention, it is still not free from controversies.

Investigators may find an early suspect who appears to fit the profile, and ignore or foreclose investigating other leads. For example, Richard Jewell was extensively investigated (and attacked in the media) following the Centennial Olympic Park bombing in Atlanta. This not only caused great distress to Jewell, but delayed identifying the true culprit, Eric Robert Rudolph. Focusing on Jewell is a false positive. The added cost of the false positive on Jewell was that FBI and local police gave up the search for other suspects for quite a while. The converse of the false positive is the false negative, when investigators are blinded by an erroneous aspect of a profile, and clear a suspect who is actually guilty. Criminals who engage in the calculating use of violence and threats of violence to trigger emotional responses such as humiliation, fear, and terror do so to coerce behavior such as obedience and submission. However, Eric Robert Rudolph exhibited traits that set him apart from typical criminals, even political terrorists, and demonstrated behavior representative of criminal sexual sadists as sex and punishment were central themes of his crimes with the focus "on domination, control, humiliation, pain, injury, and violence, or a combination of these themes, as a means to elicit suffering." The personal records of criminal sexual sadists frequently involve complex, elaborate, detailed scenarios that include specific methods of capture, control, locations, and well-planned sequence of acts which often encompass multiple victims. Former US Army explosives expert, Eric Robert Rudolph released an 11-page manifesto which detailed his accounts of bombings that killed two people and injured more than 120 others. "Among the information: that the Olympic bombing was intended to be part of a

week-long campaign of explosions aimed at shutting down the games and embarrassing the US government."

Another noted example of the failure of profiling is with the Beltway sniper attacks, where the killer was thought to be a middle-aged white male—but in fact the crimes were perpetrated by two black males, one of whom was only 17 years old.

The Peggy Hettrick murder case is controversial because it is the only documented case of an individual having been convicted due to a reversed engineered false profile and the erroneous testimony of the psychologist who developed the profile. In 1999, a jury convicted Timothy Masters of the 1987 killing of Peggy Hettrick. Masters spent over 9 years in a Colorado prison before his released on January 22, 2008 Timothy Masters was arrested and convicted of sexual murder based on the testimony of a forensic psychologist while the opinion of a Robert R. “Roy” Hazelwood, a retired FBI criminal investigative analyst was ignored. The forensic psychologist developed a psychological profile of a killer using narrative and drawings made by Masters to conclude that Masters’ supposed fantasy was the motive and behavioral preparation for the sexual murder, regardless of the fact that the forensic psychologist knew that there was no direct or physical evidence linking Masters to the crime. The cautionary lesson in the Masters case is what happens when forensic psychologists advance opinions about criminal matters based on the extrapolation of academic research on psychological concepts involving sexual homicide cases and reject the opinions of professional criminal profilers who incorporate law enforcement analysis coupled with criminal evidentiary considerations into their work.

Some experts in criminal psychology such as Brent Turvey, as quoted by journalist Malcolm Gladwell in *The New Yorker* have questioned its scientific validity. Many profilers and FBI agents are not psychologists, and some researchers who looked at their work found methodological flaws. However, if these criticisms are seen as heuristic, rather than destructive, the Gladwell article suggests otherwise.

Three psychologists from the Universities of Liverpool and Hull are questioning the basic presumption that you can draw conclusions about a person from a single instance of behaviour under such special circumstances. "The notion that particular configurations of demographic features can be predicted from an assessment of particular configurations of specific behaviors occurring in short-term, highly traumatic situations seems an overly ambitious and unlikely possibility. Thus, until such inferential processes can be reliably verified, such claims should be treated with great caution in investigations and should be entirely excluded from consideration in court."

Active profiling as allowed by the Department of Justice includes covert alteration of the environment to observe the responses of a suspect. This can be used to check whether the suspect's behavior fits the profile, but risks being labeled as police harassment or entrapment.

Popular use of the term *criminal profiler* has led to the proliferation of many self-described profilers offering their purported expert opinions on cable news shows in response to incidents capturing national attention in the United States. Such individuals usually have degrees in criminal justice or psychology but lack any law enforcement experience.

Chapter- 9

Facial Recognition System

Swiss European surveillance: facial recognition and vehicle make, model, color and license plate reader.

Side View

Close-up of the infrared illuminator. This light is invisible to the human eye but it creates a day-like environment for the surveillance cameras.

A **facial recognition system** is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

Techniques

Traditional

Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distill an image into values and comparing the values with templates to eliminate variances.

Popular recognition algorithms include Principal Component Analysis with eigenface, Linear Discriminate Analysis, Elastic Bunch Graph Matching fisherface, the Hidden Markov model, and the neuronal motivated dynamic link matching.

3-D

A newly emerging trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. This technique uses 3-D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.

One advantage of 3-D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view.

Even a perfect 3D matching technique could be sensitive to expressions. For that goal a group at the Technion applied tools from metric geometry to treat expressions as isometries

Skin texture analysis

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.

Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent.

Software

- Google's Picasa digital image organizer has a built in face recognition system starting from version 3.5 onwards. It can associate faces with persons, so that queries can be run on pictures to return all pictures with a specific group of people together. Picasaweb.com has also been providing a similar feature to its users.
- Apple iPhoto, photo organizer distributed with iLife suite of applications includes a system using which people can tag recognized people on photos. Then they can be searched using Spotlight.
- Sony's Picture Motion Browser (PMB) analyses photo, associates photos with identical faces so that they can be tagged accordingly, and differentiates between photos with one person, many persons and nobody.
- Facebook also included face recognition technology

Notable users and deployments

The London Borough of Newham, in the UK, previously trialled a facial recognition system built into their borough-wide CCTV system.

The German Federal Police use a facial recognition system to allow voluntary subscribers to pass fully automated border controls at Frankfurt Rhein-Main international airport. Subscribers need to be European Union or Swiss citizens. Since 2005 the German Federal Criminal Police Office offers centralized facial recognition on mugshot images for all German police agencies. Recognition systems are also used by casinos to catch card counters and other blacklisted individuals.

The Australian Customs Service has an automated border processing system called SmartGate that uses facial recognition. The system compares the face of the individual with the image in the e-passport microchip, certifying that the holder of the passport is the rightful owner.

Pennsylvania Justice Network searches crime scene photographs and CCTV footage in the mugshot database of previous arrests. A number of cold cases have been resolved since the system became operational in 2005. Other law enforcement agencies in the USA and abroad use arrest mugshot databases in their forensic investigative work.

U.S. Department of State operates one of the largest face recognition systems in the world with over 75 million photographs that is actively used for visa processing.

Spaceship Earth in Epcot uses this[?] for the touch screen part of the ride.

Additional uses

In addition to being used for security systems, authorities have found a number of other applications for facial recognition systems. While earlier post 9/11 deployments were well publicized trials, more recent deployments are rarely written about due to their covert nature.

At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida, used Identix' facial recognition software, FaceIt, to search for potential criminals and terrorists in attendance at the event. (it found 19 people with pending arrest warrants)

In the 2000 presidential election, the Mexican government employed facial recognition software to prevent voter fraud. Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new facial images to those already in the voter database, authorities were able to reduce duplicate registrations. Similar technologies are being used in the United States to prevent people from obtaining fake identification cards and driver’s licenses.

There are also a number of potential uses for facial recognition that are currently being developed. For example, the technology could be used as a security measure at ATM's; instead of using a bank card or personal identification number, the ATM would capture an image of your face, and compare it to your photo in the bank database to confirm your identity. This same concept could also be applied to computers; by using a webcam to capture a digital image of yourself, your face could replace your password as a means to log-in.

As part of the investigation of the disappearance of Madeleine McCann the British police are calling on visitors to the Ocean Club Resort, Praia da Luz in Portugal or the surrounding areas in the two weeks leading up to the child's disappearance on Thursday 3 May 2007 to provide copies of any photographs of people taken during their stay, in an attempt to identify the abductor using a biometric facial recognition application.

Also, in addition to biometric usages, modern digital cameras often incorporate a facial detection system that allows the camera to focus and measure exposure on the face of the subject, thus guaranteeing a focused portrait of the person being photographed. Some cameras, in addition, incorporate a smile shutter, or take automatically a second picture if someone closed their eyes during exposure.

Comparative study

Among the different biometric techniques, facial recognition may not be the most reliable and efficient. However, one key advantage is that it does not require aid (or consent) from the test subject. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd. Other biometrics like fingerprints, iris scans, and speech recognition cannot perform this kind of mass identification. However, questions have been raised on the effectiveness of facial recognition software in cases of railway and airport security.

Criticisms

Weaknesses

Face recognition is not perfect and struggles to perform under certain conditions. Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems."

Other conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low resolution images.

Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render in the system less effective. For instance: Canada now allows only neutral facial expressions in passport photos.

Effectiveness

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system having been running for several years. "Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target." This information seems to conflict with claims that the system was credited with a 34% reduction in crime - which better explains why the system was then rolled out to Birmingham also.

An experiment by the local police department in Tampa, Florida, had similarly disappointing results.

"Camera technology designed to spot potential terrorists by their facial characteristics at airports failed its first major test at Boston's Logan Airport"

Privacy concerns

Many citizens are concerned that their privacy will be invaded. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know where you are, and what you are doing, at all times. This is not to be an underestimated concept as history has shown that states have typically abused such access before.

Recent Improvements

In 2006, the performance of the latest face recognition algorithms were evaluated in the Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.

Low-resolution images of faces can be enhanced using face hallucination. Further improvements in high resolution, megapixel cameras in the last few years have helped to resolve the issue of insufficient resolution.

Early development

Pioneers of Automated Facial Recognition include: Woody Bledsoe, Helen Chan Wolf, and Charles Bisson.

During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces (Bledsoe 1966a, 1966b; Bledsoe and Chan 1965). He was proud of this work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images (in effect, a book of mug shots) and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database. Bledsoe (1966a) described the following difficulties:

> “This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations.”
>
> —Woody Bledsoe, 1966

This project was labeled man-machine because the human extracted the coordinates of a set of features from the photographs, which were then used by the computer for recognition. Using a graphics tablet (GRAFACON or RAND TABLET), the operator would extract the coordinates of features such as the center of pupils, the inside corner of eyes, the outside corner of eyes, point of widows peak, and so on. From these coordinates, a list of 20 distances, such as width of mouth and width of eyes, pupil to pupil, were computed. These operators could process about 40 pictures an hour. When building the database, the name of the person in the photograph was associated with the list of computed distances and stored in the computer. In the recognition phase, the set of distances was compared with the corresponding distance for each photograph, yielding a distance between the photograph and the database record. The closest records are returned.

This brief description is an oversimplification that fails in general because it is unlikely that any two pictures would match in head rotation, lean, tilt, and scale (distance from the camera). Thus, each set of distances is normalized to represent the face in a frontal orientation. To accomplish this normalization, the program first tries to determine the tilt, the lean, and the rotation. Then, using these angles, the computer undoes the effect of these transformations on the computed distances. To compute these angles, the computer must know the three-dimensional geometry of the head. Because the actual heads were unavailable, Bledsoe (1964) used a standard head derived from measurements on seven heads.

After Bledsoe left PRI in 1966, this work was continued at the Stanford Research Institute, primarily by Peter Hart. In experiments performed on a database of over 2000

photographs, the computer consistently outperformed humans when presented with the same recognition tasks (Bledsoe 1968). Peter Hart (1996) enthusiastically recalled the project with the exclamation, "It really worked!"

By about 1997, the system developed by Christoph von der Malsburg and graduate students of the University of Bochum in Germany and the University of Southern California in the United States outperformed most systems with those of Massachusetts Institute of Technology and the University of Maryland rated next. The Bochum system was developed through funding by the United States Army Research Laboratory. The software was sold as ZN-Face and used by customers such as Deutsche Bank and operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hair styles and glasses—even sunglasses".

In about January 2007, image searches were "based on the text surrounding a photo," for example, if text nearby mentions the image content. Polar Rose technology can guess from a photograph, in about 1.5 seconds, what any individual may look like in three dimensions, and thought they "will ask users to input the names of people they recognize in photos online" to help build a database.