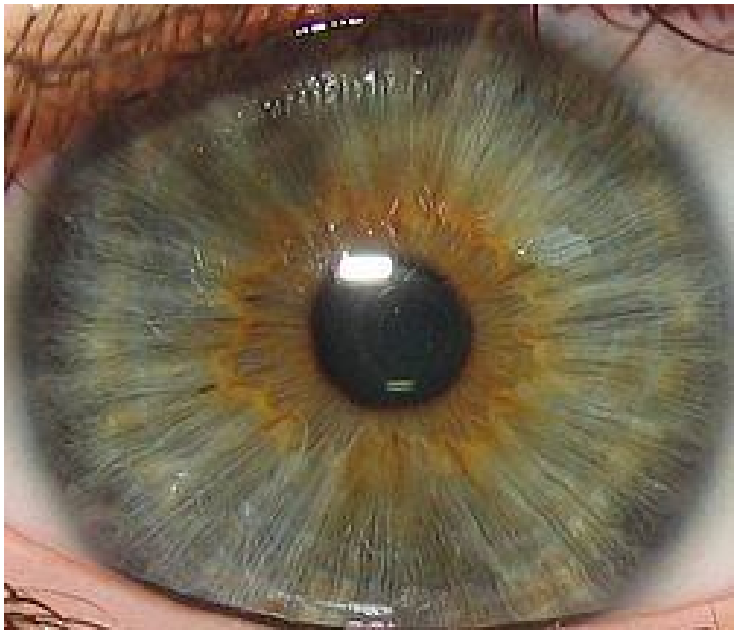
PART II

INFORMATION GATHERING AND IDENTIFICATION



The iris is just one of many biometric identifiers that Big Brother wants from you.

Do not be a frog. Wake Up! Get Smart!

EIGHT

INFORMATION GATHERING

Big Brother is not content in watching everything you do and everyplace you go. Eavesdropping on everything you say and hear is also not enough. He wants to know everything about you and he has been collecting every scrap of data about you since you were born.

National Database

Several thousand law enforcement agencies are creating the foundation of a domestic intelligence system through computer networks that analyze vast amounts of police information to fight crime and uncover terror plots. While federal authorities struggled to meet information-sharing mandates after the September 11, 2001 terrorist attacks, police agencies on the West Coast poured millions of criminal and investigative records into shared digital repositories. These data warehouses give investigators and analysts new power to discern links among people, patterns of behavior and other hidden clues.

Those network efforts will expand as other police departments connect to a fledgling Justice Department system called the National Data Exchange (N-DEx). Federal authorities hope N-DEx will become what one called a "one-stop shop," enabling federal law enforcement, counterterrorism and intelligence analysts to automatically examine the enormous caches of local and state records for the first time.[1]

The NSA call database was created by the National Security Agency starting in 2001. It contains hundreds of billions of records of telephone calls made by U.S. citizens from the four largest telephone carriers: AT&T, SBC, BellSouth (all three now being called AT&T since AT&T bought BellSouth and SBC purchased AT&T but kept the AT&T name), and Verizon.[2]

The existence of this database and the NSA program that compiled it was unknown to the general public until USA Today broke the story on May 10, 2006.[3] It is estimated that the database contains over 1.9 trillion call-detail records. According to Bloomberg News, the effort began approximately seven months before the September 11, 2001 attacks.[4]

Big Brother has hundreds of government and private sector data bases at his dispoal. In time it will be virtually impossible for a person to not have their detailed personal file available to Big Brother.

Student database

The Department of Education has taken a giant step toward creating a de facto national student database that will track students by their personal information from preschool through career. Although current federal law prohibits this, the department decided to ignore Congress and, in effect, rewrite the law. Student privacy and parental authority will suffer.

Buried deep within the American Recovery and Reinvestment Act of 2009 (stimulus bill) were provisions encouraging states to develop data systems for collecting copious information on public-school kids. To qualify for stimulus money, states had to agree to build such systems according to federally dictated standards. So all 50 states either now maintain or are capable of maintaining extensive databases on public school students.

The administration wants this data to include much more than name, address and test scores. According to the National Data Collection Model, schools are to collect information on health-care history, family income and family voting status.

Even though current federal law prohibits a nationwide student database and strictly limits disclosure of a student's personal information the Obama administration is eager to create the database.

In April of 2001 the Education Department proposed regulations that would allow it and other agencies to share a student's personal information with practically any government agency or even private company, as long as the disclosure could be said to support an evaluation of an "education program."

The proposed regulations provoked a firestorm of criticism, but on December 2, 2011, the Department of Education rejected almost all the criticisms and released the regulations. As of January 3, 2012, interstate and intergovernmental access to your child's personal information will be practically unlimited. The federal government will have a de facto nationwide database of supposedly confidential student information.

The department says this won't happen. If the states choose to link their data systems, it says, that's their business, but "the federal government would not play a role" in operating the resulting

megadatabase. The department would have access to the data systems of each of the 50 states and would be allowed to share that data with anyone it chooses, as long as it uses the right language to justify the disclosure.

Just as the department used the promise of federal money to coerce the states into developing these systems, it would almost certainly do the same to make them link their systems. The result would be a nationwide student database, whether or not it is "operated" from an office in Washington.[5]

Google collects Wi-Fi data

Google's legal problems surrounding data collection around the world intensified when it emerged that the company faces a police investigation in Australia, the latest in a growing number of countries expressing concern about the its **Street View** mapping services.

The probe, which comes amid accusations that Google breached privacy laws, was announced a day after the firm agreed to hand over data it has collected through wireless networks to French, German and Spanish authorities. Canada has also recently launched a probe into Google amid privacy concerns relating to the Street View service which uses camera-equipped fleets of cars to take 360 degree panoramic pictures for an online atlas.

In May of 2010 Google acknowledged it had **mistakenly collected** fragments of data over public and unsecured Wi-Fi networks in more than 30 countries as it was taking pictures of neighborhoods. It said it discovered the problem after German regulators launched an inquiry into the matter. [**Authors' note:** LIE!]

In the UK, the information commissioner ruled in 2009 that Google's Street View technology carries a small risk of privacy invasion but should not be stopped, although members of the public have taken direct action in at least one location to prevent the company from taking photographs on their streets. Residents in Broughton blocked the driver of a Google Street View car, which captures the photos, when it tried to enter the village, near Milton Keynes.

The Australian investigation comes as more regulators and consumers watchdogs around the world are complaining that Google does not take people's privacy seriously enough. [**Authors' note:** Google is a NSA/CIA front corporation!]

Australia's communications minister Stephen Conroy has accused Google of being responsible for the "single greatest breach in the history of privacy."

"There have been some complaints voiced … by the public in respect to practices that have been reported involving allegations that some information may have been obtained by staff of Google travelling around the streets," said Australia's federal attorney general Robert McClelland.

"In light of concerns having been raised by the public, my department thought there were issues of substance that were raised that require police investigation." The case was referred to the Australian federal police on Friday, he said. It will focus on whether the company breached the country's telecommunications interceptions act, which prevents people accessing electronic communications other than for authorized purposes.

The US Federal Trade Commission has already begun an informal inquiry into the matter and Google has said it would co-operate with authorities. Suits have been filed in Washington, California, Massachusetts and Oregon by people who accuse Google of violating their privacy by collecting data from open Wi-Fi networks. On its official blog Google has said that the software code responsible for collecting the data was **used by mistake**, and that all Street View cars were grounded when the mistake was discovered.[5] [**Authors' note**: LIE!]

Google is a NSA/CIA front corporation. It is conducting illegal data collection and surveillance for the NSA/CIA. When it gets caught the heat is on Google instead of the NSA/CIA which are two of Big Brother's illegal/criminal spy agencies.

Google believes it is Big Brother

Google CEO Eric Schmidt believes that if you are concerned about Google retaining your personal data, then you must be doing something you should not be doing. "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place," Schmidt told CNBC.

He explained that everything Google collects is subject to government snooping. "If you really need that kind of privacy, the reality is that search engines – including Google – do retain this information for some time and it's important, for example, that we are

all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities."[6]

Google thinks it is Big Brother because it is. Google is not Big Brother by itself, but it is an integral part of Big Brother.

Google tracks your web searches

Google, MSN Search, Yahoo, AOL, and most other search engines collect and store records of your search queries. If these records are revealed to others, they can be embarrassing or even cause great harm. Would you want strangers to see searches that reference your online reading habits, medical history, finances, sexual orientation, or political affiliation?[7]

Google tracks your web history

The FBI is pressing Internet service providers to record which Web sites customers visit and retain those logs for two years, a requirement that law enforcement believes could help it in investigations of child pornography and other serious crimes.

FBI Director Robert Mueller supports storing Internet users' "origin and destination information," a bureau attorney said at a federal task force meeting in February 2010. As far back as a 2006 speech, Mueller had called for data retention on the part of Internet providers, and emphasized the point two years later when explicitly asking Congress to enact a law making it mandatory. But it had not been clear before that the FBI was asking companies to begin to keep logs of what web sites are visited.

The FBI is not alone in renewing its push for data retention. As CNET reported in February 2010, a survey of state computer crime investigators found them to be nearly unanimous in supporting the idea. Matt Dunn, an Immigration and Customs Enforcement agent in the Department of Homeland Security, also expressed support for the idea during the task force meeting.

Greg Motta, chief of the FBI's digital evidence section, said it was trying to preserve its existing ability to conduct criminal investigations. Federal regulations in place since at least 1986 require phone companies that offer toll service to "retain for a period of 18 months" records including "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call."[8]

Google voluntarily complied with the FBI request and keeps track of every web site you visit if you use its browser. Anyone who uses Google Chrome web browser can go to the Google web site and look up their surfing history.[9]

Google admits that it keeps track of what books you read on Google Books, but claims it keeps the information for a "limited period of time to enforce viewing limits."[10]

Google and Microsoft admit they keep track of every search users make.[11] Let Google speak for itself:

> **Why does Google store search engine logs data?**
>
> We store this data for a number of reasons. Most importantly, we store data to improve our search results and to maintain the security of our systems. Analyzing logs data helps our engineers both improve your search quality and build helpful innovative services. Take the example of Google Spell Checker. Google's spell checking software automatically looks at a user's query and checks to see if that user is using the most common version of the word's spelling. If we calculate a user is likely to get more relevant search results with an alternative spelling, we'll ask "Did you mean: (more common spelling)?" In order to provide this service, we study the data in our logs. Logs data also helps us improve our search results. If we know that users are clicking on the #1 result, we know we're probably doing something right, and if they're hitting next page or reformulating their query, we're probably doing something wrong. In addition, logs data helps us prevent against fraud and other abuses, like phishing, scripting attacks, and spam, including query click spam and ads click spam.
>
> **Why are search engine logs kept before being anonymized?**
>
> We strike a reasonable balance between the competing pressures we face, such as the privacy of our users, the security of our systems and the need for innovation. We believe anonymizing IP addresses after 9 months and cookies in our search engine logs after 18 months strikes the right balance.[12]

Google is an intricate part of Big Brother. It keeps all data forever. Google and other search engine providers keep track of your searches and create a profile which it sells to advertizers. Google makes millions of federal reserve notes doing this, but it also gives Big Brother this

information. It dutifully turns over information upon request from governments.[13]

We also believe that virtually all the information Google and other web companies collect is handed over to Big Brother because he created them. He uses it to create a complex profile of everyone who uses search engines with information from other sources such as web surfing, educational records, medical records, criminal record, voting record, traffic citations, work history, financial history, credit rating, purchases, library checkout records, telephone calls, televison/cable viewing, associations with people, churches, political parties, organizations and whatever else it can accumulate.

Acxiom

Acxiom is a global interactive marketing services company that uses consumer data, analytics, information technology, data aggregation, data integration, and consulting solutions to help companies conduct direct marketing programs. Acxiom's interactive capabilities allow marketers to have direct interaction and response with consumers, and these services include direct-mail, e-mail, mobile advertising, display advertising, social media, and Web-site personalization.

It has been described as "one of the biggest companies you've never heard of."[14] In addition to collecting detailed information about people, the company helps marketers anticipate the future needs of consumers, according to the documentary "The Persuaders." As the **world's largest processor of consumer data**,[15] Acxiom has identified 70 types of consumers with its segmentation product PersonicX.

Forrester Research considers Acxiom "a technology powerhouse" with deep industry expertise across a multitude of industries. Acxiom has traditionally been known for helping many of the world's largest financial services companies conduct direct marketing campaigns, but now more than 75 percent of its revenue is derived from non-financial services clients. Today, Acxiom is a $1.38 billion-a-year company, representing more than 12 percent of the direct-marketing-services sector's $11 billion in estimated annual sales.

Acxiom has offices in several states in America, but it also has offices in the United Kingdom, France, Germany, Netherlands, Portugal, Poland, Australia, China and Brazil. Its services are also available to companies in scores of other countries.[16]

Acxiom is a big Big Brother corporation that few have ever heard of. It has files on virtually everyone in America. Big Brother can access its files any time he wants to.

Law enforcement

FBI Joint Terrorism Task Force

A flyer was passed out in the Phoenix, Arizona area requesting law enforcement officers to keep a sharp lookout for American citizens which the NJTTF believes are "domestic terrorists." They are patriots who do not want to see America fall prey to the New World Order Gang and their world dictatorship.

According to the "Protecting America: National Task Force Wages War on Terror" press release of August 19, 2008, there "are 106 FBI Joint Terrorism Task Forces around the country, where local, state, and federal agencies work together to combat terrorism on a regional scale.

"Coordinating the efforts of all those regional task forces is the National Joint Terrorism Task Force, a fusion of local, state, and federal agencies acting as an integrated force to combat terrorism on a national and international scale.

The National Joint Terrorism Task Force, or NJTTF, was established in 2002 to manage the burgeoning Joint Terrorism Task Force program—the number of task forces almost doubled overnight, from 35 pre-9/11 to 56 soon after 9/11 (50 more have been established since then). Of course, JTTFs have been around since the 1980s, starting in New York and Chicago.

Originally located at FBI Headquarters, the NJTTF moved to the multi-agency National Counterterrorism Center (NCTC), where it performs its mission while also working with NCTC personnel to exchange information, analyze data, and plan anti-terrorism strategies.

So what exactly is the NJTTF's mission? Managing the Bureau's JTTFs around the country is major part of the operation, and it's a huge job—there are currently more than 4,000 JTTF task force members from over 600 state and local agencies as well as 50 federal agencies.

According to Special Agent Gregory Massa, who heads the NJTTF, "We support each task force in every way imaginable – from sharing intelligence and terrorism threat information to providing big-picture terrorism analysis…from offering guidance and oversight to setting sound program policies… from supplying resources for manpower, equipment, and space to facilitating training."

Another vital aspect of the NJTTF's mission is sharing information among its 80 members – officers, agents, and analysts – who then pass the information onto the 48 different agencies they represent. Those agencies – from the law enforcement, intelligence, homeland security, defense, diplomatic, and public safety sectors – Include the Department of Homeland Security, the U.S. military, and federal, state, and local partners. Men and women from the U.S. Secret Service, Federal Air Marshals, New York City Police Department, Naval Criminal Investigative Service, Federal Bureau of Prisons, Amtrak Police, and dozens of other organizations work together every day in the global war on terrorism.

NJTTF members are also working together on joint initiatives designed to address broader terrorism threats. For example:

Operation TRIPWIRE focuses on information and intelligence-sharing operations from the NJTTF's participating agencies to help identify terrorist sleeper cells in the U.S.

Correctional Intelligence Initiative assists JTTFs and correctional facilities to combat prison radicalization and recruitment of prisoners within federal, state, local, tribal, and territorial prisons.

Rail Liaison Agent Program works to protect the country's critical mass transit and freight rail infrastructure by collecting and disseminating rail-related terrorism intelligence info to JTTFs and critical rail partners nationwide.

Military Working Group is comprised of 12 Department of Defense agencies who look at military-specific terrorism threats.

The NJTTF and the JTTFs work tirelessly to protect Americans from terrorism, but they can't do it alone. Says Agent Massa, "Every law enforcement officer, first responder, military member, intelligence analyst, and private citizen has a role to play in the global war on terror." And he asks that suspicious activity of any kind be reported to your local JTTF or FBI field office.[17]

Police download data from your cell phone

The Michigan State Police have been using devices capable of downloading text messages, address books and other data from cell phones.

The Data Extraction Devices are commonly used to transfer data from an old cell phone to a new one, but they are also used by law enforcement for obtaining information such as erased text messages.

Police said they are using the devices in certain criminal cases, but after obtaining a search warrant or with the cell phone owner's consent. "The implication by the ACLU that the (state police) uses these devices 'quietly to bypass Fourth Amendment protections against unreasonable searches' is untrue, and this divisive tactic unjustly harms police and community relations," the state police said. The devices cost around $3,000 each, and the Michigan State Police have five.[18]

Big brother has been stealing data from cell phones for years. Eventually laws will be passed giving the minions of Big Brother the "authority" to steal any and all data from cell phones, laptops, iPads, desktop computers, etc.

The way to keep Big Brother from stealing your personal data is to not keep any on your e-devices. Keep all private data on flash drives or portable hard drives. Sell your fancy cell phones, iPhones, Smartphones, etc. and get a cheap cell phone with a camera. Do NOT keep pictures or personal information, phone numbers and data on the cell phone. **Memorize** your important phone numbers or keep them in an old fashion address book. If you must have a fancy cell phone get a flash drive that can be attached and keep all of your personal data on it.

WAKE UP AMERICA! GET SMART!

UK phone and email database

A new Big Brother database holding the telephone numbers and email accounts of everyone in Britain would raise serious data protection concerns.

Prime Minister Gordon Brown signaled plans to bring in the database holding details of every phone call, email and time spent on the internet by the public in last month's draft Queen's Speech. The proposal is part of Government plans to implement a European Union directive which was brought in after the July 7, 2005 bombings to encourage uniform record-keeping across EU states.

Information commissioner Richard Thomas warned the database would be "a step too far for the British way of life." "Do we really want the police, security services and other organs of the state to have access to more and more aspects of our private lives?" he asked. "There needs to be the fullest public debate about the justification for, and

implications of, a specially-created database – potentially accessible to a wide range of law enforcement authorities – holding details of everyone's telephone and internet communications."

The danger of Big Brother having a record of everything everyone has ever said or written is frightening. A government or renegade bureaucrat could use a inappropriate statement by an individual to discredit or blackmail him.

Commissioner Thomas also cited the expansion of the DNA database and the centralized collection and retention of data from Automatic Number Plate Recognition roadside cameras as two examples of other intrusive Big Brother programs. "Before major new databases are launched careful consideration must be given to the impact on individuals' liberties and on society as a whole," he cautioned. "Sadly, there have been too many developments where there has not been sufficient openness, transparency or public debate."

The fear of information being stolen or lost is real. There were a number of high profile data losses in 2008 including the loss by HM Revenue and Customs of the details of over 25 million families.[19]

Homeland Security tracks your air travel

The Department of Homeland Security keeps a record of every flight everyone in America makes.

Starting in the mid-1990s, many airlines handed over passenger records to the government. Since 2002, the government has mandated that the commercial airlines deliver this information routinely and electronically.[20]

Be careful what you read

International travelers concerned about being labeled a terrorist or drug runner by secret Homeland Security algorithms may want to be careful what books they read on the plane. Newly revealed records show the government is storing such information indefiniely.[21]

Biometric database

FBI and States Vastly Expand DNA Databases

Law enforcement officials are vastly expanding their collection of DNA to include millions more people who have been arrested or

detained but not yet convicted. The move is raising concerns about the privacy of petty offenders and people who are presumed innocent.

Until now, the federal government genetically tracked only convicts. But starting in April of 2009, the Federal Bureau of Investigation (FBI) will join 15 states that collect DNA samples from those awaiting trial and will collect DNA from detained immigrants.

The F.B.I., with a DNA database of 6.7 million profiles, expects to accelerate its growth rate from 80,000 new entries a year to 1.2 million by 2012 – a 15-fold increase. Criminal justice experts cite Fourth Amendment privacy concerns and worry that the nation is becoming a genetic surveillance society.

Britain may provide a window into America's genetic surveillance future: As of March 2008, 857,000 people in the British database, or about one-fifth, have no current criminal record. In December, the European Court of Human Rights ruled that Britain violated international law by collecting DNA profiles from innocent people, including children as young as 10.[22]

The Newborn Screening Saves Lives Act

On April 24, 2008, President signed into law: S. 1858, the "Newborn Screening Saves Lives Act of 2007," which authorizes through fiscal year 2012 new and existing programs at the Department of Health and Human Services concerning newborn screening. Sen. Christopher Dodd [D-CT] sponsored the bill and two of the co-sponsors were Sen. Edward Kennedy and Hillary Clinton.

The bill violates the U.S. Constitution and the Nuremberg Code, writes Twila Brase, president of the Citizen's Council on Health Care (CCHC). "The DNA taken at birth from every citizen is essentially owned by the government, and every citizen becomes a potential subject of government-sponsored genetic research," she states. "It does not require consent and there are no requirements to inform parents about the warehousing of their child's DNA for the purpose of genetic research. Already, in Minnesota, the state health department reports that 42,210 children of the 780,000 whose DNA is housed in the Minnesota 'DNA warehouse' have been subjected to genetic research without their parents' knowledge or consent."

S.1858 is justified by the federal government as a "national contingency plan" in that it represents preparation for any sort of public health emergency. The bill states that the federal government should

"continue to carry out, coordinate, and expand **research in newborn screening**" and "maintain a **central clearinghouse** of current information on newborn screening... ensuring that the **clearinghouse** is available on the Internet and is updated at least quarterly." Sections of the bill also make it clear that DNA may be used in genetic experiments and tests.

All 50 states are now routinely providing results of genetic screenings to the Department of Homeland Security and this bill will establish the legality of that practice plus include DNA.[23]

The government has your baby's DNA

Newborn babies in the United States are routinely screened for a panel of genetic diseases. Since the testing is mandated by the government, it is often done without the parents' consent, according to Brad Therrell, director of the National Newborn Screening & Genetics Resource Center. In many states babies' DNA is stored indefinitely, according to the resource center.

DNA samples are kept so that tests can be repeated, if necessary, and in case it is ever needed to help parents identify a missing or deceased child. The samples are also used for medical research.

Art Caplan, a bioethicist at the University of Pennsylvania, says he understands why states do not first ask permission to screen babies for genetic diseases. "It's paternalistic, but the **state** has an **overriding interest** in protecting these babies."

Genetic testing for newborns started in the 1960s with testing for diseases and conditions that, if undetected, could kill a child or cause severe problems, such as mental retardation. Since then, the screening has helped save countless newborns.

Over the years, many other tests were added to the list. Now, states mandate that newborns be tested for anywhere between 28 and 54 different conditions, and the DNA samples are stored in state labs for anywhere from three months to indefinitely, depending on the state.[24]

Obama backs national DNA database

In an interview aired March 6, 2010 on "America's Most Wanted," Barak Obama expressed strong agreement as host John Walsh extolled the virtues of collecting DNA at the time of an arrest and putting it into a single, national database.

"We have 18 states who are taking DNA upon arrest," Walsh said. "It's no different than fingerprinting or a booking photo. ... Since those states have been doing it, it has cleared 200 people that are innocent from jail."

"It's the right thing to do," Obama replied. "This is where the **national registry** becomes so important, because what you have is individual states – they may have a database, but if they're not **sharing it** with the state next door, you've got a guy from Illinois driving over into Indiana, and they're not talking to each other."

"It's a horrible idea – tremendously invasive," said Bill Quigley of the Center for Constitutional Rights, who also disputed Walsh's claim that DNA is no different from fingerprints.

In 2004, California ballot measure requiring DNA testing for all felony arrests and for some misdemeanor arrests. New York City Mayor Michael Bloomberg wants DNA tests for everyone arrested in the city, even for misdemeanors. Just days before Obama took office, the Bush administration implemented a 2006 law to take DNA from federal arrestees, including immigration detainees.

In 2006, then Senator Obama filed S. 109-3822 and in 2007 he filed S. 110-976 – legislation that would create a national DNA database. The same bill was filed by Sen. Patrick Kennedy in 2008 (S. 110-6498). All three bills died in the Senate.[25]

Big Brother will eventually have a massive international DNA database. He wants your DNA and he will not stop until he gets it.

Israel to be first to create biometric database for all citizens

The government of Israel approved a motion in 2008 calling for the establishment of a biometric database by the Ministry of Interior and the Public Security Ministry.

The motion, dubbed the "identification card, travel papers and biometrics database bill," became "The Biometric Database Law" (Hebrew: חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009) and was passed in 2009.

It gives the Israeli government the authority to collect fingerprints and facial features from all Israeli residents, and imbed the biometric information into identity cards and passports. It also gave the government the authority to create a biometric database of all citizens and residents.

The data is being used by the Ministry of Interior to create "smart," forgery-proof identification papers and passports.

Internal Security Minister Avi Dichter told the government that the "need to create a unique (physical) bond between the person carrying an ID and the data which appears on it, is essential in order to fight the worldwide forgeries… Should we succeed we would be able to create a nationwide database controlled, as it should be, by the State."

The existence of such a database – which includes every citizen – has yet to be sanctioned in any Western country.[26]

National fingerprint registry

Buried in the text of the revised legislation, approved by the Senate Banking Committee by a 19-2 vote in March 2008, is a plan to create a new national fingerprint registry. It covers just about everyone involved in the mortgage business, including lenders, "loan originators," and some real estate agents.

What's a little odd is the lack of public discussion about this new fingerprint database. No mention of it appears in the official summary of the revised Senate bill that was introduced by Diane Feinstein (D-Ca.) and Mel Martinez (R-Fl.). No copy of the revised Senate legislation is posted on the Library of Congress' Thomas Web site, which is the usual procedure.

The federal fingerprint database requires any "loan originator" to furnish "fingerprints for submission to the Federal Bureau of Investigation" and a wealth of other unnamed government agencies. Loan originator is defined as someone who accepts a residential mortgage application, negotiates terms on a mortgage, advises on loan terms, prepares loan packages, or collects information on behalf of the consumer.

Some states already have fingerprinting requirements. Colorado, Kansas, Mississippi, and Montana require "mortgage brokers" to get fingerprinted.

In the proposed federal system, what remains unclear is what happens to the fingerprints once submitted. The legislation talks about a "background check" which creates a Nationwide Mortgage Licensing System and Registry. The bill does specify that the registry will be run by the Conference of State Bank Supervisors and the American Association of Residential Mortgage Regulators. Those two groups are currently developing a "central repository" of information with

document collecting and fingerprinting that "will be accessed through a secure Web site over the Internet."[27]

Boston launches flu shot tracking

Using technology originally developed for mass disasters, Boston disease trackers embarked on a novel experiment in 2008 aimed at creating a citywide registry of everyone who has had a flu vaccination.

Everyone who participates will get a bracelet printed with a unique identifier code. Information about the recipient and the shot will be entered into handheld devices similar to those used by delivery truck drivers.

"Anything you can do to better pinpoint who's vaccinated and who's not, that's absolutely vital," said Michael Osterholm, director of the Center for Infectious Disease Research & Policy at the University of Minnesota. "I wish more cities were doing this kind of thing."

Boston is believed to be the first city to embrace this particular approach to tracking vaccinations against the seasonal flu, estimated to kill 36,000 people each year in America.[28]

Data mining/sharing

Government bureaucrats want to know every transaction that everyone in America makes. They are gathering and sharing as much information as possible about everyone in America. They say it is to help them prevent terrorists from launching more attacks against the American people. This is true, but this information can also be used to manipulate people or control them. Eventually it could be used by a world dictator to give him absolute control over everyone on Earth.

MATRIX

The Multistate Anti-Terrorism Information Exchange Program, also known by the acronym "MATRIX," was a federally funded data mining system originally developed for the Florida Department of Law Enforcement.

The system analyzed government and commercial databases to find associations between suspects or new suspects. The database and technologies used in the system were housed by Seisint, a Florida-based company since acquired by Lexis Nexis.

The Matrix program was shut down in June 2005 after federal funding was cut in the wake of public concerns over privacy and state surveillance. The amount of information that was being compiled on millions of people was astounding. The MATRIX allegedly gathered information about a person's criminal history, driver's license data, vehicle registration records, and public data record entries, credit history, driver's license photographs, marriage and divorce records, social security number, date of birth, and the names and addresses of family members, neighbors and business associates. The ACLU argued that the type of data that the MATRIX compiles could be expanded to include information in commercial databases encompasses such as purchasing habits, magazine subscriptions, income and job history.[29]

JRIES

The Joint Regional Information Exchange System (JRIES) began in December 2002 as an all-source intelligence/information sharing system. It was initially designed to connect the California Anti-Terrorism Information Center, the New York Police Department, and the Defense Intelligence Agency (DIA). These groups designed JRIES, which was first deployed in February 2003, to facilitate the exchange of suspicious activity reports, register events potentially related to terrorist activity, and foster real-time intelligence and law enforcement collaboration in a secure environment across federal, state, and local jurisdictions. The system provided a simple and efficient way for the law enforcement community to obtain situational awareness concurrently, without the need for hundreds of phone calls. In 2003 the DIA relinquished control to the Department of Homeland Security. As of 2004, about 100 law enforcement organizations were using JRIES.[30]

RISS

Regional Information Sharing Systems (RISS) is an information-sharing program funded by the U.S. Federal government whose purpose is to connect databases from local and regional law enforcement so that they can use each other's data for criminal investigations.[31]

In 1997, RISS created RISSNET, a network to interconnect many local, state, regional, and tribal law enforcement databases. In 2002, RISSNET was connected with the FBI's Law Enforcement Online

system. In 2003, the National Criminal Intelligence Sharing Plan (NCISP) declared that RISSNET would be the official "backbone" for all unclassified, but sensitive criminal intelligence data traffic. Later that year, members were also given access to the Automated Trusted Information Exchange (ATIX) database, which contains information on homeland security and terrorist threats.[32]

HSIN

The Homeland Security Information Network (HSIN) is a web-based platform, run by the Department of Homeland Security, which is designed to allow local, state, tribal, and federal government agencies to share "Sensitive But Unclassified (SBU)" information with each other over a secure channel.[33]

NCISP

The National Criminal Intelligence Sharing Plan (NCISP) is an intelligence-sharing initiative that links the computer databases of local, state, regional, tribal law enforcement agencies with those of the U.S. federal government.[34]

Government agencies and corporations have detailed files on millions of Americans. The information in those files will grow larger, and they will be shared by numerous government agencies and corporations. The lives of most Americans are an open book. Knowledge is power, and having knowledge of people's habits will give power-mongers greater advantage over them.

Big Brother is building a massive data gathering network with numerous agencies and private corporations. He is gathering and storing as much information about everyone on Earth that he can. Information is power and the more he gets the more powerful he becomes. If you want to keep your personal information to yourself pull out of the Big Brother information web.

Feds tracking credit cards without warrant

Federal law enforcement routinely tracks individuals through their credit cards, cell phones, car rentals and even store customer loyalty programs without obtaining a warrant, an online privacy activist has discovered.

According to a document obtained from the Department of Justice by privacy activist Christopher Soghoian, federal agents working on a criminal investigation can draw up their own paperwork requesting that credit companies and retailers give the agents real-time access to purchases made by a particular person. No court reviews these orders, and the only role courts play in the process is to issue a non-disclosure order to the retailer or credit card company involved, meaning the **person being tracked will never be notified of the surveillance**.

The process is known as a "hotwatch," and it can be used to spy on cell phones, credit card use, purchases at stores when a customer loyalty card is used, car rentals, and flight ticket purchases. The process "sidestep[s] any Fourth Amendment protections," Soghoian writes.

"A search of Google, Lexisnexis and Westlaw revealed nothing related to 'hotwatch' orders, and so I filed a FOIA request to find out more," Soghoian writes. "If the government 'routinely' applies for and obtains hotwatch orders, why wasn't there more information about these?"

A year-and-a-half and an appealed decision later the Justice Department released a document outlining "hotwatches."[35]

NSA to store yottabytes of surveillance data in Utah megarepository

The National Security Agency is constructing a datacenter in the Utah desert that they project will be storing yottabytes of surveillance data. There are a thousand gigabytes in a terabyte, a thousand terabytes in a petabyte, a thousand petabytes in an exabyte, a thousand exabytes in a zettabyte, and a thousand zettabytes in a yottabyte. A yottabyte is 1,000,000,000,000,000 gigabytes.

What with millions of phones being tapped and all data duplicated, constant recording of all radio traffic, 24-hour high definition video surveillance by satellite, there's terabytes at least of data coming in every day. And who knows when you will have to sift through August 2007's overhead footage of Baghdad for heat signatures in order to confirm some other intelligence?

A commentor pointed out that in the study cited, yottabytes are only one possible estimate for total storage requirements. The more realistic estimates are in the hundreds of petabytes, which is much easier for a datacenter to accommodate.[36]

Big Brother has virtually unlimited storage space and he plans to collect every piece of data in the world and use software programs to analyze that data. Big Brother wants to be God and he will not stop until YAHWEH stops him. In the meantime we can resist him.

How NSA access was built into Windows

A Careless mistake by Microsoft programmers has revealed that special access codes prepared by the National Security Agency (NSA) have been secretly built into Windows.

The NSA access system is built into every version of the Windows operating system now in use, except early releases of Windows 95 (and its predecessors). The discovery comes close on the heels of the revelations earlier this year that another US software giant, Lotus, had built an NSA "help information" trapdoor into its Notes system, and that security functions on other software systems had been deliberately crippled.

The first discovery of the new NSA access system was made in 1997 by British researcher Dr. Nicko van Someren. But it was only in early 1999 that a second researcher rediscovered the access system. With it, he found the evidence linking it to NSA.

Computer security specialists have been aware for two years that unusual features are contained inside a standard Windows software "driver" used for security and encryption functions. The driver, called ADVAPI.DLL, enables and controls a range of security functions. If you use Windows, you will find it in the C:\Windows\systemdirectory of your computer.

Dr. Nicko van Someren reported at last year's Crypto 98 conference that he had disassembled the ADVADPI driver. He found it contained two different keys. One was used by Microsoft to control the cryptographic functions enabled in Windows, in compliance with US export regulations. But the reason for building in a second key, or who owned it, remained a mystery.

Andrew Fernandez, chief scientist with Cryptonym of Morrisville, North Carolina, had been probing the presence and significance of the two keys. Then he checked the latest Service Pack release for Windows NT4, Service Pack 5. He found that Microsoft's developers had failed to remove or "strip" the debugging symbols used to test this software before they released it. Inside the code were the labels for the two keys.

One was called “KEY.” The other was called “NSAKEY.” Later a third key was found.

Fernandes reported his re-discovery of the two CAPI keys, and their secret meaning, to “Advances in Cryptology, Crypto’99” conference. According to those present at the conference, Windows developers attending the conference did not deny that the “NSA” key was built into their software. But they refused to talk about what the key did, or why it had been put there without users’ knowledge.

According to Fernandez of Cryptonym, the result of having the secret key inside your Windows operating system “is that it is tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once these security services are loaded, they can effectively compromise your entire operating system.” The NSA key is contained inside all versions of Windows from Windows 95 OSR2 onwards.

Dr. van Someren feels that the primary purpose of the NSA key inside Windows may be for legitimate US government use. But he says that there cannot be a legitimate explanation for the third key in Windows 2000 CAPI. “It looks more fishy,” he said.

Fernandez believes that NSA’s built-in loophole can be turned round against the snoopers. A demonstration “how to do it” program that replaces the NSA key can be found on Cryptonym’s website.[37]

UK Interception Modernization Program

United Kingdom’s Home Office says all data from the web could be stored in giant government database dubbed the Interception Modernization Program (IMP).

Internet “black boxes” will be used to collect every email and web visit in the UK under the government’s plans for a giant “big brother” database.

Further details of the planned database emerged at a 2008 meeting of internet service providers (ISPs) in London where representatives from BT, AOL Europe, O2 and BSkyB were given a PowerPoint presentation of the issues and the technology surrounding the IMP, the name given by the Home Office to the database proposal.

Whitehall experts working on the IMP unit told the meeting the security and intelligence agencies wanted to use the stored data to help fight serious crime and terrorism, and said the technology would allow them to create greater “capacity” to monitor all communication traffic

on the internet. The “black boxes” are an attractive option for the internet industry because they would be secure and not require any direct input from the ISPs.[38]

Big Brother will set up massive data bases in every country on Earth and then connect them to form one super data base with which he can access information about anyone, any company or organization.

Travel records kept by DHS

The Department of Homeland Security (DHS) collects and stores a great deal of information on everyone who flies into and out of America.

According to the blog Philosecurity, DHS-member agency Customs and Border Protection (CBP) stores a surprising amount of personal information on international travelers underneath its Automated Targeting System (ATS) which began in the mid-1990s.

International travelers flying into or out of the United States can expect this information to be collected and stored by DHS:

Credit card number and expiration
IP address used to make web travel reservations
Hotel information and itinerary
Full name, birth date, and passport number
Full airline itinerary, including flight numbers and seat numbers
Cruise ship itinerary
Phone numbers, including business, home, and cell
Every frequent flyer and hotel number associated with the subject, even ones not used for the specific reservation

According to a DHS Privacy Impact Assessment from 2006, CBP collects such personally identifiable information because it enhances the agency’s “ability to identify possible violations of U.S. law or other threats to national security would be critically impaired without access to this data.” The program also collects and stores information regarding land border crossings as well as people involved with the import and export of cargo.

Nearly two years ago, the Washington Post reported that the ATS database held much more information than previously revealed by the federal government, including what travelers **brought to read** during their trip.

The Post also told of one gentleman, Zakariya Reed, who has been stopped at the border at least seven times in approximately one year's time. During two of those stops, the CBP officers questioned Reed about "politically charged" op-eds he wrote for his local paper that were critical of U.S. foreign policy in the Middle East. Once, during a secondary screening interview, officers "had them printed out on the table in front of me," Reed told the Post.[39]

End Game

ADAMS

Anomaly **D**etection at **M**ultiple **S**cales (**ADAMS)** is a $35 million DARPA project designed to identify patterns and anomalies in very large data sets. It is under DARPA's Information Innovation office and began in 2011.[40-43] The project is intended to detect and prevent insider threats such as "a soldier in good mental health becoming homicidal or suicidal," an "innocent insider becoming malicious," or a "a government employee [whom] abuses access privileges to share classified information."[41, 44] Specific cases mentioned are Nidal Malik Hasan and Wikileaks alleged source Bradley Manning.[45] Commercial applications may include finance.[45] The intended recipients of the system output are operators in the counterintelligence agencies.[41, 44]

The Proactive Discovery of Insider Threats Using Graph Analysis and Learning (PRODIGAL) is part of the ADAMS project.[44, 46] The Georgia Tech team includes noted high-performance computing researcher David A. Bader.[47-48]

PRODIGAL

Proactive **D**iscovery of **I**nsider Threats Using **G**raph **A**nalysis and **L**earning (PRODIGAL) is a computer system for predicting anomalous behavior of people by data mining network traffic such as emails, text messages and log entries.[49] It is part of DARPA's Anomaly Detection at Multiple Scales (ADAMS) project.[50] The initial schedule is for two years and the budget $9 million.[51]

It uses graph theory, machine learning, statistical anomaly detection, and high-performance computing to scan larger sets of data more quickly than in past systems. The amount of data analyzed is in the range of terabytes per day.[51] The targets of the analysis are employees within the government or defense contracting organizations; specific

examples of behavior the system is intended to detect include the actions of Nidal Malik Hasan and Wikileaks alleged source Bradley Manning.[49] Commercial applications may include finance.[49] The results of the analysis, the five most serious threats per day, go to agents, analysts, and operators working in counterintelligence.[49, 51-52]

The research is being carried out by:

Georgia Institute of Technology College of Computing
Georgia Tech Research Institute
Defense Advanced Research Projects Agency
Army Research Office
Science Applications International Corporation
Oregon State University
University of Massachusetts
Carnegie Mellon University[53]

How will a person who is arrested or grabbed by Big Brother be able to defend himself against the accusation that he planned to commit a terrorist act? Will he be given his day in court or will be be thrown in a military prison or concentration camp and never heard from again as Senate bill 1867 (The National Defense Authorization Act) allows for? Will be he tortured and eventually killed from abuse by Big Brother?

Total Information Awareness

Privacy and civil-rights groups have hailed the decision by Congress to kill a controversial Pentagon program to construct a powerful computerized surveillance system that would lead to unprecedented spying into the private lives of Americans. The program, "Total Information Awareness," had its name changed to "Terrorist Information Awareness." It was created by Ronald Reagan's national security adviser, retired Admiral John Poindexter, who was convicted of five felony counts of lying to Congress about the Iran-Contra affair in the mid-1980s.[54]

The program had a name change, but government bureaucrats can still use the technology to spy on law-abiding citizens. This technology could be used in the future by a world dictator to watch what everyone does and says.

"The personal computer may soon be not-so-private, with the United States and some European nations working on laws allowing them access to search the content held on a person's hard drive."[55]

Lifelog

LifeLog was a project of the Information Processing Technology Office of the Defense Advanced Research Projects Agency According to its bid solicitation pamphlet, it was to be "an ontology-based (sub)system that captures, stores, and makes accessible the flow of one person's experience in and interactions with the world in order to support a broad spectrum of associates/assistants and other system capabilities." The objective of the "LifeLog" concept was "to be able to trace the 'threads' of an individual's life in terms of events, states, and relationships."

"LifeLog aims to compile a massive electronic database of every activity and relationship a person engages in. This is to include credit card purchases, web sites visited, the content of telephone calls and e-mails sent and received, scans of faxes and postal mail sent and received, instant messages sent and received, books and magazines read, television and radio selections, physical location recorded via wearable GPS sensors, biomedical data captured through wearable sensors, The high level goal of this data logging is to identify "preferences, plans, goals, and other markers of intentionality."

The DARPA program was canceled in 2004 after criticism from civil libertarians concerning the privacy implications of the system, but it may be operating in secret.[56]

Technology eventually will be developed and implemented that can record everything a person sees, says, hears and even thinks. People will also be tracked wherever they go, and a record will be kept of every place they visit and everyone they encounter. Every detail of a person's life will become the property of Big Brother's government bureaurats.

MyLifeBits

MyLifeBits is a Microsoft Research project inspired by Vannevar Bush's hypothetical Memex computer system. The project includes full-text search, text and audio annotations, and hyperlinks. The "experimental subject" of the project is computer scientist Gordon Bell, and the project will try to collect a lifetime of storage on and about Bell. Jim Gemmell of Microsoft Research and Roger Lueder were the architects and creators of the system and its software.

Computerologists are seeking the Holy Grail of computer technology – recording every byte of a person's life from birth to death

and be able to access any moment in time by date or subject. They are in the infancy of this technology but within two decades they may have the hardware and software to make it a practical option for consumers. For information about this technology see the footnote.[57]

Big Brother is working feverishly to develop this technology and make it mandatory for everyone on Earth to wear a video camera that will record everything one sees, hears and says. That information will be downloaded every 24 hours via the Internet or satellite and stored in massive databases in every country. Those databases will be accessible by Big Brother. He will also have software that will enable him to access anyone's lifelog by date or subject matter. He will also be able to access live feeds from specific individuals if he so desires.

Big Brother is also working on technology that will enable him to record every thought that a person has and store those thoughts in massive databases and retrieve any thought any time he chooses.

If Big Brother attains this ability he will be god-like. That is what he wants – to be God Almighty, BUT he will NEVER be God. Instead the final Big Brother (the Antichrist) will come to an abrupt end after a brief reign of just seven years as world dictator. At the Second Advent of Jesus Christ he will be slain (Daniel 7.11), resurrected and cast alive into the Lake of Fire (Revelation 19.20) where he will spend all eternity being punished with literal fire and brimstone, burning wind, burning coals, unquenchable thirst and myriad other physical torments (Psalm 11.6; 140.10; Proverbs 25.22; Luke 16.24; Romans 12.20; Revelation 14.9-11; 20.10).

Amazon's Big Brother patent will enable it to know where you will go

An Amazon patent, made public in December 2011, will allow Amazon to track, through mobile devices, where individuals have been, and determine where they are likely to go next to send them ads, coupons, or other messages that could appear on a mobile phone or on displays that individuals are likely to see on their routes.

The patent which was granted on December 6, 2011, was submitted in March 2007. The language of the patent is a bit bureaucratic, but decipherable:

> A system, comprising: a processor; and a memory coupled to the processor, wherein the memory comprises program instructions executable by the processor to: determine one or more locations a

> user of a mobile device has visited on a current path; predict a next destination for the user of the mobile device based on the one or more locations the user of the mobile device has visited on the current path, wherein to predict the next destination, the program instructions are further executable to: predict a plurality of likely destinations, and receive one or more bids for communicating advertising content regarding one or more of the likely destinations for the user of the mobile device, wherein the next destination corresponds to a likely destination for which a selected bid was received; and communicate advertising content to a display device other than the mobile device located along the current path between a current location for the mobile device and the next destination.

The system calculates a path and then predicts a set of likely next destinations. It then takes bids from third parties that want to send marketing messages to displays along the route the person takes, monitoring speed and direction to time displays for maximum chance of visibility. Ads can also be sent to a person's mobile device and messages telling the person to look over at a particular display as depicted in the science fiction movie "Minority Report."

According to the patent's description, location could be specific spots inside a mall:

> In some embodiments, mobile device users' current and past travel patterns may be analyzed to determine a predicted next destination. For instance, by analyzing the recent movements of a mobile device user among stores in a shopping mall, it may be determined that a particular store is a predicted next destination for the mobile device user. Thus, advertising content for the predicted destination, such as coupons, may be sent to the mobile device user.[58]

Sometime in the next decade or two this advertizing technology will be implemented in the Western world and then throughout the planet. People will be bombarded with advertisements everytime they step out of their homes. That is only the commercial end of this fantastic plan. Big Brother will use the technology to predict where people will go when they leave home, what they will do and what they will buy. Big Brother does not just want to watch your every move and eavesdrop on everything you say he wants to know what you plan to do before you do it. His ultimate goal will be to read your mind 24-7.

Retroactive surveillance

According to the Brookings Institution, authoritarian governments will soon be able to perform retroactive surveillance on anyone within their borders.

These regimes will store every phone call, instant message, email, social media interaction, text message, movements of people and vehicles and public surveillance video and they will search through it at their leisure. This hideous fact was explained in detail in "Recording Everything: Digital Storage as an Enabler of Authoritarian Government," written by John Villaseno, a senior fellow at Brookings and a professor of electrical engineering at UCLA.[59]

This technology will allow bureaucrats to shadow a person's movements and communications before he became an alleged "enemy of the state." "For example, if an anti-regime demonstrator previously unknown to security services is arrested, it will be possible to go back in time to scrutinize the demonstrator's phone conversations, automobile travels, and the people he or she met in the months and even years leading up to the arrest," the report says. "These enormous databases of captured information will create what amounts to a surveillance time machine. ... This will fundamentally change the dynamics of dissent, insurgency and revolution."

Villaseno noted that when the government of Libya fell, insurgents found equipment that had captured 30 to 40 million minutes of phone conversations per month and enabled the government to read activist emails. There have been reports that the government of Syria wants to build communications intercepts as well.

Key to this possibility is the dramatic drop in the cost of storage. In 1984 it cost an amazing $85,000 to store just one gigabyte, and today it costs five cents per gigabyte.

In 2015 the cost of storing all the phone calls made in a year by an average person will be less than 2 cents. In Red China 500,000 video cameras will be installed throughout the city of Chongquing. By 2020, all that video could be stored for 25 cents per Chongquing resident per year. Total costs of surveillance – gathering, aggregating, managing, analyzing – will be greater, but as Big Data becomes a reality, tools for handling it will become better and cheaper.

"Many of the solutions that are being developed in the commercial world for searching and analyzing data could be applied to state-sponsored surveillance as well," Villaseno noted. "Awareness of the

likelihood that all messages – including those that are encrypted – will eventually be read by security services will chill dissent."

The main vendors that sell this technology are Blue Coat, Cisco, Huawei, NetApp, Qosmos (France) and Utimaco (Germany).[60]

Big Brother will definitely examine as much surveillance data as possible to find political dissidents he may have passed by. He will also manufacture surveillance data to frame dissidents.

Conclusion

Big Brother wants every scrap of information about you that he can get. You must actively deny him this information. Do NOT give out personal information, DNA, fingerprints or any biometric information to the state or a company. Find a way to opt out and if there is no way do without the service or product. You can resist Big Brother!

Notes

1. O'Harrow, Robert, Jr. and Nakashima, Ellen. "National Dragnet Is a Click Away." Washington Post. 3.06.2008. A01. www.washingtonpost.com/wp-dyn/content/article/2008/03/05/AR2008030503656_ pf.html.

2. www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

3. http://en.wikipedia.org/wiki/National_Criminal_Intelligence_Sharing_Plan.

4. Shane, Scott. "Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11." New York Times. 6.30.2006. www.nytimes.com/2007/10/14/business/14qwest.html?_r=1.

5. Emmett McGroarty, Jane Robbins. How the feds are tracking your kid." 12.28.2011. www.nypost.com/p/news/opinion/opedcolumnists/how_the_feds_are_tracking_your_kid_xC6wecT8ZidCAzfqegB6hL.

6. Davies, Caroline. "Google investigated by Australian police over Wi-Fi data collection: Google Street View cars around the world mistakenly collected Wi-Fi data." Guardian. 6.06.2010. www.guardian.co.uk/technology/2010/jun/06/google-privacy-data-collection-street-view

7. Metz, Cade. "Google chief: Only miscreants worry about net privacy." The Register. 12.07.2009. www.theregister.co.uk/2009/12/07/schmidt_on_privacy.

7. http://bigbrotherxposed.com/page15.html#SAFESEARCHES.

8. "Six Tips to Protect Your Search Privacy." Electronic Frontier Foundation. September 2006. www.eff.org/wp/six-tips-protect-your-search-privacy.

9. McCullagh, Declan. "FBI wants records kept of Web sites visited." Cnet.com. 2.05.2010. http://news. cnet.com/8301-13578_3-10448060-38.html.

10. www.lifehack.org/articles/productivity/track-internet-history-on-any-computer.html.

11. http://books.google.com/support/bin/answer.py?hl=en&answer=43733.

12. http://forums.canadiancontent.net/computers-internet/80817-did-you-know-microsoft-google.html.

13. www.google.com/intl/en/privacy/faq.html.

14. www.google.com/transparencyreport/governmentrequests.

15. Frontline "The Persuaders." 11.09.2004. www.pbs.org/wgbh/pages/frontline/shows/persuaders/etc/script.html.

16. Behar, Richard. "Never Heard Of Acxiom? Chances Are It's Heard Of You. How a little-known Little Rock company – the world's largest processor of consumer data – found itself at the center of a very big national security debate." CNN. 2.23.2004. http://money.cnn.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm.

17. www.acxiom.com.

18. www.fbi.gov/news/stories/2008/august/njttf_081908.

19. Stern, Andrew and Woodall, Bernie. "Michigan police and ACLU in flap over cell phone downloads." Daily Press. 4.21.2011. www.dailypress.com/news/nationworld/sns-rt-usreport-us-michigatre 73k5cb-20110421,0,5821147.story.

20. Hope, Christopher. "'Big Brother' database of all phone calls and emails condemned by watchdog. 8.17.2008. www.telegraph.co.uk/news/newstopics/politics/lawandorder/2403908/Big-Brother-database-of-all-phone-calls-and-emails-condemned-by-watchdog.html.

21. O'Neill, Sean. "Is this useful information or a waste of time?" http://travel.yahoo.com/p-interests-24971907.

22. Singel, Ryan. "U.S airport screeners are watching what you read." 9.20.2007. www.wired.com/politics/onlinerights/news/2007/09/flight_tracking.

23. Moore, Solomon. "F.B.I. and States Vastly Expand DNA Databases." 4.18.2009. www.nytimes.com/2009/04/19/us/19DNA.html.

24. 15. AAPS News. "President Bush Signs S. 1858 into Law." 4.28.2008. www.whitehouse.gov/news/releases/2008/04/20080424-17.html. & www.govtrack.us/congress/bill.xpd?bill=s110-1858 & www.aaps online.org/newsoftheday/0025. & www.naturalnews.com/z025116.html. & Donovan, Patty. "The Bill Nobody Noticed: National DNA Databank." 12.18.2008. www.govtrack.us/congress/bill.xpd?bill=s110-1858.

25. Cohen, Elizabeth. "The government has your baby's DNA." CNN. 3.04.2010. www.cnn.com/ 2010/HEALTH/02/04/baby.dna.government/index.html?hpt=Sbin.

26. Gerstein, Josh. "President Obama backs DNA test in arrests." 3.09.2010. www.politico.com/news/stories/0310/34097.html.

27. Somfalvi, Attila. "Israel to be first in world to create biometric database for all citizens ynetnews, 8.03.2008. Attila Somfalvi www.ynetnews.com/articles/0,7340,L-3577046,00.html.

28. McCullagh, Declan. "Housing bailout bill creates national fingerprint registry." CNET. 3.23.2008. http://news.cnet.com/8301-13578_3-9951420-38.html.

29. Smith, Stephen. "Boston launches flu shot tracking." Boston.com. 11.21.2008. www.boston.com/news/local/massachusetts/articles/2008/11/21/boston_launches_flu_shot_tracking.

30. Ramasastry, Anita. Find Law. 11.05.2003. http://writ.news.findlaw.com/ramasastry/20091229.html.

31. http://en.wikipedia.org/wiki/Joint_Regional_Information_Exchange_System.

32. www.riss.net.

33. www.riss.net/overview.aspx.

34. www.dhs.gov/files/programs/gc_1156888108137.shtm & www.fema.gov/emergency/nrf/HSIN.htm.

34. http://en.wikipedia.org/wili/Homeland_Security_Information_Network.

35. http://en.wikipedia.org/wiki/National_Criminal_Intelligence_Sharing_Plan.

36. Tencer, Daniel. “Feds tracking credit cards, store purchases without warrants.” Raw Story. 12.03.2010. www.rawstory.com/rs/2010/12/feds-credit-cards-without-warrant. & www.scribd.com/doc/44542244/DOJ-powerpoint-presentation-on-Hotwatch-surveillance-orders-of-credit-card-transactions.

37. Coldewey, Devin. “NSA to store yottabytes of surveillance data in Utah megarepository,” Crunch Gear. 11.01. www.crunchgear.com/2009/11/01/nsa-to-store-yottabytes-of-surveillance-data-in-utah-mega repository.

38. Campbell, Duncan. 4.09.1999. www.heise.de/tp/r4/artikel/5/5263/1.html.

39. Verkaik, Robert. Independent, 11.05.2008. www.independent.co.uk/news/uk/home-news/govern ment-black-boxes-will-collect-every-email-992268.html.

40. Harwood, Matthew. “The Information DHS Stores on International Travelers.” 9.10.2009. www.securitymanagement.com/news/information-dhs-stores-international-travelers-006185.

40. http://philosec urity.org/2009/09/07/what-does-dhs-know-about-you.

40. www.washingtonpost.com/wp-dyn/content/article/2007/09/21/AR2007092102347.html.

41. “ADAMS.” DARPA Information Innovation Office. www.darpa.mil/Our_Work/I2O/Programs/Anomaly_Detection_at_Multiple_Scales_(ADAMS).aspx.

42. “Anomaly Detection at Multiple Scales (ADAMS) Broad Agency Announcement DARPA-BAA-11-04.” General Services Administration. 2010-10-22. https://www.fbo.gov/download/2f6/2f6289e99a0c04942bbd89ccf242fb4c/DARPA-BAA-11-04_ADAMS.pdf.

43. Ackerman, Spencer. “Darpa Starts Sleuthing Out Disloyal Troops.” Wired. 10.11.2011. www.wired.com/dangerroom/2010/10/darpa-starts-sleuthing-out-disloyal-troops.

44. Keyes, Charley. “Military wants to scan communications to find internal threats.” CNN. 10.27.2010. http://articles.cnn.com/2010-10-27/us/pentagon.e.mail.profiling_1_nidal-hasan-darpa-fort-hood.

45. “Georgia Tech Helps to Develop System That Will Detect Insider Threats from Massive Data Sets.” Georgia Institute of Technology. 11.10.2011. www.gatech.edu/newsroom/release.html?nid=72599.

46. “Video Interview: DARPA’s ADAMS Project Taps Big Data to Find the Breaking Bad.” Inside HPC. 2011-11-29. http://insidehpc.com/2011/11/29/video-interview-darpas-adams-project-taps-big-data-to-find-the-breaking-bad.

47. Brandon, John. “Could the U.S. Government Start Reading Your Emails?” Fox News. 12.03.2011. www.foxnews.com/scitech/2011/12/03/could-us-government-start-reading-your-emails.

48. “Anomaly Detection at Multiple Scales.” Georgia Tech College of Computing.

49. http://en.wikipedia.org/wiki/Anomaly_Detection_at_Multiple_Scales.

50. “Video Interview: DARPA’s ADAMS Project Taps Big Data to Find the Breaking Bad.” Inside HPC. 2011-11-29. http://insidehpc.com/2011/11/29/video-interview-darpas-adams-project-taps-big-data-to-find-the-breaking-bad.

51. Brandon, John. “Could the U.S. Government Start Reading Your Emails?” Fox News. 12.03.2011. www.foxnews.com/scitech/2011/12/03/could-us-government-start-reading-your-emails.

52. “Georgia Tech Helps to Develop System That Will Detect Insider Threats from Massive Data Sets.” Georgia Institute of Technology. 10.11.2011. www.gatech.edu/newsroom/release.html?nid=72599.

53. Storm, Darlene. “Sifting through petabytes: PRODIGAL monitoring for lone wolf insider threats.” Computer World. 12.06.2011. http://blogs.computer world. com/19382/sifting_through_petabytes_prodigal_monitoring_for_lone_wolf_insider_ threats.

54. http://en.wikipedia.org/wiki/Proactive_Discovery_of_Insider_Threats_Using_ Graph_Analysis_and_Learning.

55. Lobe, Jim. “Congress Defunds Controversial ‘Total Information’ Program.” OneWorld.net. 9.26.2003. www.commondreams.org/headlines03/0926-02.htm.

56. Russia Today. “A not-so-private PC.” 3.26.2009. www.russiatoday.com/ Sci_Tech/2009-03-26/A_not-so-private_PC.html.

57. http://en.wikipedia.org/wiki/DARPA_LifeLog. & http://web.archive.org/web/ 20030603173339/http%3a//www.darpa.mil/ipto/Solicitations/PIP_03-30.html.

58. http://research.microsoft.com/en-us/projects/mylifebits/default.aspx.

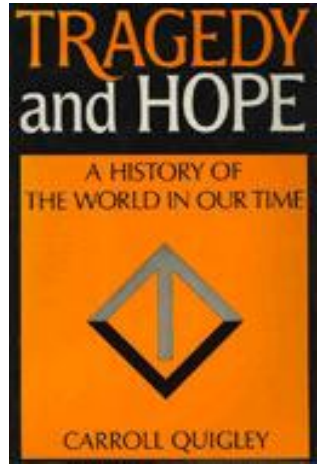
58. Wolf, Gary. “The Data-Driven Life.” NY Times. 4.28.2010. www.nytimes. com/2010/05/02/magazine/02self-measurement-t.html.

58. “Lifelogging, An Inevitability.” 2.21.2007. The Technium. www.kk.org/the technium/archives/2007/02/lifelogging_an.php.

59. Sherman, Erick. Amazon Big Brother patent knows where you'll go.” CBS News. 12.14.2011. www.cbsnews.com/8301-505124_162-57342567/amazon-big-brother-patent-knows-where-youll-go.

60. www.brookings.edu/~/media/Files/rc/papers/2011/1214_digital_storage_vill asenor/1214_digital_storage_villasenor.pdf.

61. Greene, Tim. “Coming soon: Ubiquitous surveillance from Big Brother’s wayback machine.” NetworkWorld. 12.15.2011. www.networkworld.com/news/2011 /121511-government-surveillance-254137.html?hpg1=bn.

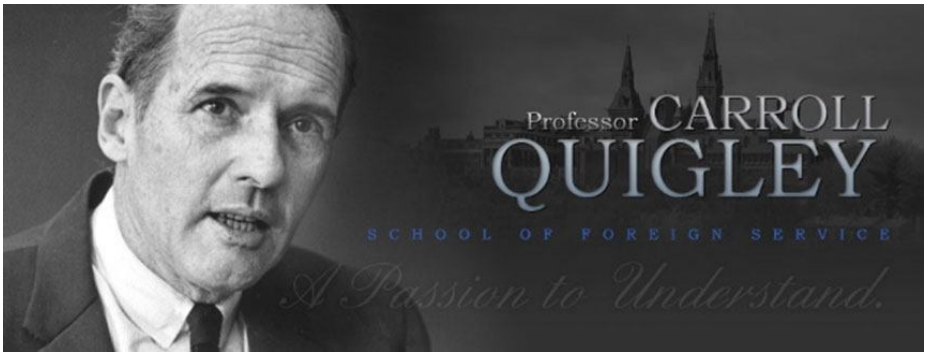


www.carrollquigley.net/pdf/ Tragedy_and_Hope.pdf

NINE

IDENTIFICATION PROGRAMS

Big Brother wants to gather and collate every shred of information and every biometric piece of data about you including your DNA.



> But, in general, his **freedom and choice will be controlled** within very narrow alternatives by the fact that he will be **numbered from birth** and followed, **as a number**, through his educational training, his **required military** or **public service**, his **tax contributions**, his health and medical requirements, and his final retirement and death benefits. (Quigley, Carroll, *Tragedy and Hope*, p. 866, emphasis added)

ID Cards

Biometric Social Security Card

New York Democrat Senator Chuck Schumer and South Carolina Republican Senator Lindsey Graham, presented an immigration bill that includes a proposal to issue a biometric ID card to all working Americans that would contain physical data such as fingerprints or retinal scans.

The "enhanced Social Security card" is being touted as a way to curb illegal immigration by giving employers the power to quickly and accurately determine who is eligible to work. "If you say [illegal

immigrants] can't get a job when they come here, you'll stop it," Schumer told the Wall Street Journal. Proponents also hope legal hiring will be easier for employers if there's a single go-to document instead of the 26 that new employees can currently use to show they're authorized to work.

A similar program run by the Department of Homeland Security, in which 1.4 million transportation workers have been issued biometric credentials, required applicants pay $132.50 to help cover the costs of the initiative.[1]

Big Brother will eventually force everyone in America to get a SS card with biometric identifiers in it. Passports and driver's licenses will also have biometrics in them and within a decade or so everyone in America will be required to get a National ID Card loaded with biometrics.

Patriots who opt out of the Big Brother program will not be able to collect Social Security benefits or receive any federal or state benefit. We will also not be able to get jobs, travel by plane, train or bus and we will not be able to get a passport. Patriots will be prisoners in America.

India launches universal ID system with biometrics

India launched an ambitious program to fit each of its 1.2 billion residents with an Unique Identification Number (UID). Each number is tied into three pieces of bio-metric data: fingerprints (all ten), iris scans (both eyes), and a picture of the face.

Starting in September of 2010, the Unique Identification Authority of India (UIDAI) began processing people in various locations around the country. While residents are not mandated to get a UID, a growing list of services including social welfare and even some bank accounts will soon require the identification number. If successful, this will be the first biometrically verified universal ID implemented on a national scale.

There is some chilling Big Brother-like aspects to this whole affair. Yet the problem of insuring that resources make it to India's poor is very real, and there is the strong possibility that the UID will be empowering and democratizing to the 440 million Indians below the poverty level.[2]

Big Brother intends to compel the politicians and bureaucrats of every nation on Earth to issue a national ID card to every citizen and illegal alien. After a national ID card has been issued to virtually

everyone on Earth the implantable computer chip will replace it. That day is only a couple decades away.

People's Republic of China

The identity card contains basic information regarding the individual, such as the following:

Obverse side:

Full name – in Chinese characters only. Non-Chinese ethnic names and foreign names are transliterated into Chinese. First-generation ID cards contained handwritten names for rare Chinese characters, whilst the second-generation cards exclusively used computer-printed text in a larger font compared to that of the first generation, and do not support rarer characters.
Gender – containing one character for either male or female.
Ethnicity – as officially listed by the People's Republic of China.
Date of birth – listed in the Gregorian calendar format, in YMD order.
Domicile – the individual's permanent residence as dictated by the Identity Card Bill of the People's Republic of China.
Identification number
Photo of the individual

Reverse side:

Issuing authority (first-generation cards utilised a stamp; second-generation cards display text only)
The limits to validity of the document (for individuals under 16 years of age: five years; for individuals between 16 and 25 years of age: ten years; for individuals between 26 and 45 years of age: twenty years; for individuals over 46 years of age: long-term)

1 1 0 1 0 2/Y Y Y Y M M D D/8 8 8/X
Address code Date of Birth code Order code Checksum

Information stored in the identity database for biometric ID cards documents information such as work history, educational background,

religion, ethnicity, police record, medical insurance status, landlord's phone number and personal reproductive history.[3]

ID badges

Texas students test electronic eye

Some schools in Texas have begun monitoring student arrivals and departures using technology similar to that used to track livestock and pallets of retail shipments.

The Spring Independent School District is equipping 28,000 students with ID badges containing computer chips that are read when the students get on and off school buses. The information is fed by wireless phone to the police and school administrators.

In a variation on the concept, a Phoenix school district in November is starting a project using fingerprint technology to track when and where students get on and off buses. Last year, a charter school in Buffalo began automating attendance counts with computerized ID badges – one of the earliest examples of what educators said could become a widespread trend.[4]

Iris scanners

This technology will become commonplace

Homeland Security to test iris scanners

The Homeland Security Department plans to test futuristic iris scan technology that stores digital images of people's eyes in a database.

The DHS conducted a two-week test in October of 2010 of commercially sold iris scanners from Global Rainmakers Inc., at a

Border Patrol station in McAllen, Texas. The test cameras that take photos from three or four feet away, including one that works on people as they walk by, were used on illegal immigrants, said Arun Vemury program manager at the department's Science and Technology branch.

"The test will help us determine how viable this is for potential (department) use in the future," Vemury said.

Iris scanners are little used, but a new generation of cameras that capture images from six feet away instead of a few inches has sparked interest from government agencies and financial firms, said Patrick Grother, a National Institute of Standards and Technology computer scientist.

In 2007, the U.S. military began taking iris scans of thousands of Iraqis to track suspected militants. The technology was used in about 20 U.S. airports from 2005 to 2008 to identify passengers in the Registered Traveler program, who could skip to the front of security lines.[5]

Global Rainmakers, Inc. is a company founded by Hector Hoyos in Puerto Rico in 2006 (www.globalrainmakersinc.com).

Iris scanning to secure Leon, Mexico

The million-plus citizens of Leon, Mexico became the first example of a city secured through the power of biometric identification.

Iris and face scanning technologies from Global Rainmakers, Inc. will allow people to use their eyes to prove their identity, withdraw money from an ATM, get help at a hospital, and even ride the bus. GRI's eye scanning systems are not more secure than others on the market, but they are faster. Large archway detectors using infrared imaging can pick out 50 people per minute, even as they hustle by at speeds up to 3.3 mph.

The first phase of the Leon iris and face scanning project began in 2010. It is estimated to cost around $5 million and focuses on law enforcement agencies' **security check points**. Over the next three years commercial uses will be rolled out with banks leading the charge.

We have to put this in a larger context, too. India just launched its enormous effort to digitally identify more than a billion residents using fingerprints, face, and iris scans. Japan already uses finger scans during entry into the country and the European Union is working on a variety of passive scanning technologies to help secure airports and other public spaces.

Government and commercial institutions will endeavor to create enormous shared databases of biometric data and scan huge numbers of private citizens everywhere they go. The first phase of the project in Leon is going to help track the movements of "watch-listed individuals."

What is the future of this technology? Jeff Carter, chief business development officer of GRI, explained what is coming in an interview with Fast Company's Austin Carr:

> …we've even worked with three-letter agencies on technology that can capture 30-plus feet away. In certain spaces, eventually, you'll be able to have maybe one sensor the size of a dime, in the ceiling, and it would acquire all of our irises in motion, at a distance, hundreds–probably thousands as computer power continues to increase–at a time… if you've been convicted of a crime, in essence, this will act as a digital scarlet letter. If you're a known shoplifter, for example, you won't be able to go into a store without being flagged. For others, boarding a plane will be impossible."[6]

Iris scanning is just one biometric identifier Big Brother seeks to make ubiquitous. Other forms are facial recognition, fingerprints, heat signature, and DNA.

Police to use iPhone iris scans

Dozens of police departments nationwide are gearing up to use a tech company's already controversial iris- and facial-scanning device that slides over an iPhone and helps identify a person or track criminal suspects.

The "biometric" technology, which seems to take a page from TV shows like "MI-5" or "CSI," could improve speed and accuracy in some routine police work in the field. However, its use has set off alarms with some who are concerned about possible civil liberties and privacy issues.

The smartphone-based scanner, named Mobile Offender Recognition and Information System, or MORIS, is made by BI2 Technologies in Plymouth, Massachusetts, and can be deployed by officers out on the beat or back at the station.

An iris scan, which detects unique patterns in a person's eyes, can reduce to seconds the time it takes to identify a suspect in custody. This

technique also is significantly more accurate than results from other fingerprinting technology long in use by police, BI2 says.

When attached to an iPhone, MORIS can photograph a person's face and run the image through software that hunts for a match in a BI2-managed database of U.S. criminal records. Each unit costs about $3,000.

Some experts fear police may randomly scan the population, using potentially intrusive techniques to search for criminals, sex offenders, and illegal aliens. Experts also say that before police administer an iris scan, they should have probable cause a crime has been committed.

"What we don't want is for them to become a general surveillance tool, where the police start using them routinely on the general public, collecting biometric information on innocent people," said Jay Stanley, senior policy analyst with the national ACLU in Washington, D.C.

Facial recognition technology is not without its problems, however. For example, some U.S. individuals mistakenly have had their driver's license revoked as a potential fraud. The problem, it turns out, is that they look like another driver and so the technology mistakenly flags them as having fake identification.

Roughly 40 law enforcement units nationwide will soon be using the MORIS, including Arizona's Pinal County Sheriff's Office, as well as officers in Hampton City in Virginia and Calhoun County in Alabama.[7]

Iris scan

The New York-based biometric security company Hoyos Group will market an iris scanner that connects to a personal computer.

The device allows users to log into their online banking, social networks and emails – all in the blink of an eye. Hoyos unveiled their new security product, dubbed EyeLock, at the Finovate financial technology conference in May of 2011, amid claims that it is the first and only portable iris-scanning device for consumers.

The device, which is the size of a standard business card and weighs about four ounces connects to the user's computer by a USB cable. Once the accompanying software package is installed and configured, all the user needs to do to is wave the scanner in front of his eye to automatically log in to any password-protected application or website.

"Every time you log in, it reads your iris and creates a unique key, which is a series of numbers, and this key changes every time you log

in, so no one can hack it," explained Tracy Hoyos, assistant marketing director.

According to Miss Hoyos, the security offered by iris scans trumps fingerprints which have around 18 unique points while irises have 2,000.

The EyeLock will cost $99 (£60), but no release date has yet been announced. The company has already marketed another iris-scan product used in airport security and is researching ways to expand the service to other areas, including mobile phones.[8]

Iris-scanning for frequent fliers is cut back in the UK

At the very time long passport control procedures are being blamed for long delays, most iris recognition scanners have been closed with no indication they are to re-open soon.

Iris recognition scanners were introduced at several British airports in recent years to allow grequent fliers to skip the traditional immigration controls at security gates. Yet in 2011 seven of the nine facilities for new applicants to sign up for the fast-track system were closed. The scanners themselves remain open. Yet with users of the system being required to renew their records every two years, even the estimated 385,000 current users are threatened by the office closures, meaning the number of people being forced to wait in long lines for conventional passport security will increase.[8b]

This is just a minor setback for the technology. When the incompetent British bureaucrats get their act together they will expand the fast-track program and eventually require everyone entering the United Kingdom to undergo iris scanning along with fingerprinting, DNA testing, voice identification and other forms of identification. A decade or two from now people entering any nation will be scrutinized to the max. Big Brother may even require them to go through a verbal screening process in which lie detection technology will be used to determine if they are telling the truth. This technology is currently being used in Israel and will make its way to every nation in the bot too distant future.

Retinal scans

The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex

structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern.

Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric. Advocates of retinal scanning have concluded that it is so accurate that its error rate is estimated to be only one in a million.[9]

The idea for retinal identification was first conceived by Dr. Carleton Simon and Dr. Isadore Goldstein and was published in the New York State Journal of Medicine in 1935.[10] The idea was a little before its time, but once technology caught up, the concept for a retinal scanning device emerged in 1975. In 1976, Robert "Buzz" Hill formed a corporation named EyeDentify, Inc., and made a full-time effort to research and develop such a device. In 1978, specific means for a retinal scanner was patented, followed by a commercial model in 1981.[11]

Facial recognition

USA, UK, Super Bowl, banks, etc.

Facial recognition systems (FRS) are being used around the world to identify known criminals. It is one biometric identification system that does not require assistance from the subject, and it can be used to screen people entering buildings, sporting events or walking down the street.

The Pennsylvania Justice Network searches crime scene photographs and CCTV footage in the mug shot database of previous arrests. Since its use in 2005 it has helped solve several cases that were very cold. The Tampa Police Department in Florida had no success when it used FRS in a trial, and Boston's Logan Airport also failed to produce results. The Department of State operates one of the largest FRS in the world with over 75 million photographs that is actively used for visa processing.

The London Borough of Newham uses it in its CCTV system. Unfortunately the police have failed to identify a single criminal since its use in 2004. Germany uses it to allow voluntary subscribers to pass fully automated border controls at the Frankfurt Rhein-Main

international airport. The Australian Customs Service has an automated border processing system called SmartGate that uses it.

Facial recognition systems have been tested at public events. At Super Bowl XXXV in January 2001, police in Tampa Bay, Florida, used the Identix facial recognition software, FaceIt, to search for potential criminals and terrorists. It found 19 people with pending arrest warrants. Some casinos use it to identify card counters and other blacklisted individuals.

Banks may soon use FRS for identification at ATMs instead of passwords, and some companies may use it for purchases on line. Consumers would supply a photo to each vendor, and use a web cam to log-in. If banks use them for ATMs they will also use them at the teller's window.

In 2006, the performance of the latest face recognition algorithms were evaluated in the Face Recognition Grand Challenge. 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.[12]

The makers of the FRS have big dreams of how their technology can be used. They envision registers in retail stores being equipped with cameras that would take pictures of customers. The camera would be the primary means of identifying the customer, and if visual identification failed, the customer could complete the purchase by using a PIN (personal identification number). After the cash register had calculated the total sale, the face recognition system would verify the identity of the customer and the total amount of the sale would be deducted from the customer's bank account.

Face-based retailing would provide convenience for retail customers, since they could go shopping simply by showing their faces, and there would be no need to bring credit or debit cards, checks or cash. The FRS could also be used in gas stations, restaurants, movie theaters, car rental companies, hotels, amusement parks, stadiums, arenas, concerts and everyplace where financial transactions are made.[13]

It is highly probable that in the future FRS will be connected to every cash register. Yet it is not the ultimate goal of Big Brother. He wants to put a computer chip in everyone on Earth that will have RFID

technology in it so it can be read by billions of RFID readers scattered around the world in stores, buildings, offices, homes and on pedestrian walkways. He also wants to put a GPS transponder in it that can be tracked by satellite anywhere on Earth. That chip will have numerous biometric information in it such as facial scan, retina scan, fingerprints, DNA and body odor.

Facial Recognition used by nightclub

A Melbourne nightclub installed facial recognition software in April of 2009 to stamp out thugs and known troublemakers.

Chasers nightclub in Chapel St., which already has metal detectors to screen patrons for weapons, believes the system is one of the first in the world for nightclubs. Management now wants the technology to be adopted in other nightclubs to create a security network.

Melbourne's Lord Mayor Robert Doyle said the technology could help the fight against violence, and should be looked at for venues on their last warnings.

On entering, patrons' faces are scanned by a camera and the image and driver's license details are stored on computer for 28 days. If someone banned from the club tries to enter, their face comes up with a red mark, alerting security to a problem.

Chasers owner Martha Tsamis, who also owns Inflation on King St., said the $16,000 system was bought after an ammonia cocktail bomb, the effect of which is similar to mace, was set off last year. "The only way we could track people who do such things is with this, if they don't have a criminal record," Ms. Tsamis said. "The reports we have had, especially from females, is they are very happy because they know our system is there to protect people."

The Herald Sun revealed that police want hi-tech ID scanning equipment installed at all late-night city venues. A submission by Victoria Police to the Government will ask for scanners to be compulsory for "high-risk" nightclubs.[14]

Before long Big Brother will require all commercial businesses to install facial recognition technology. This will enable him to track what stores, businesses, etc. that each individual visits. It will also be handy in catching political dissidents or individuals who are living outside of the system. If an outsider has his face scanned and there is no match in Big Brother's world database the person will be detained by security or police. When Big Brother gets his tyrannical identification net in place

outsiders will not be able to freely move about. They will only be able to go outside of their hiding place at night and they will not be able to walk in any location that has spy cameras. If their face can be captured by a spycam the facial recognition software will be able to identify them. If no match is made Big Brother will know the person is an outsider and seek to have him arrested. Life for outsiders will be extremely difficult. They will not be able to make purchases of any kind and if stopped by authorities they will be detained and tossed into a concentration camp or prison.

Brazilian police use facial recognition cameras

A small camera fitted to the glasses of a police officer can capture 400 facial images per second and send them to a central computer database storing up to 13 million faces.

The camera will generally be used to scan faces in crowds up to 50 metres (164ft) away but can be adjusted, if searching for a specific target, to recognise faces as far as 12 miles away.

The system can compare biometric data at 46,000 points on a face and will immediately signal any matches to known criminals or people wanted by police. If there is a match a red signal will appear on a small screen connected to the glasses, alerting the police officer of the need to take further action or make an arrest. The devices are being tested at football matches and concerts by police in Brazil and will be used extensively at the 2014 World Cup to be held in Brazil in 2014.

Military Police officials from Sao Paulo and Rio de Janeiro, which will both host key games in the World Cup, have been given demonstrations of how the device works. Major Leandro Pavani Agostini, of Sao Paulo's Military Police, explained the benefits of the technology: "It's something discreet because you do not question the person or ask for documents. The computer does it. To the naked eye two people may appear identical but with 46,000 points compared, the data will not be beaten."

He said the device will be useful to police trying to monitor many different locations and events, ranging from airports and bus terminals to concerts and football matches. "I can insert into the database a supporter who was involved in a brawl on the field and even with the old images, he can be located in the future," he added.[15]

This technology was depicted in the Robocop films. It is only a matter of time before it will be standard equipment for most police

officers around the world. Political dissidents will have a hard time going out in public without being caught.

Voice identification

Voiceprint identification can be defined as a combination of both aural (listening) and spectrographic (instrumental) comparison of one or more known voices with an unknown voice for the purpose of identification or elimination. Developed by Bell Laboratories in the late 1940s for military intelligence purposes, the modern-day forensic utilization of the technique did not start until the late 1960s following its adoption by the Michigan State Police. From 1967 until the present, more than 5,000 law enforcement related voice identification cases have been processed by certified voiceprint examiners.

It has been used in a variety of criminal cases, including murder, rape, extortion, drug smuggling, wagering-gambling investigations, political corruption, money-laundering, tax evasion, burglary, bomb threats, terrorist activities and organized crime activities. It is part of a larger forensic role known as acoustic analyses, which involves tape filtering and enhancement, tape authentication, gunshot acoustics, reconstruction of conversations and the analysis of any other questioned acoustic event.[16]

Vascular technology

Vein matching, also called **vascular technology**,[17] is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the skin.[18] Though used by the Federal Bureau of Investigation and the Central Intelligence Agency,[19] 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.[18, 20]

Walk identification

Big Brother scientists are working on technology that will enable Big Brother to identify people by the way they walk.

Abstract – We propose a view-based approach to recognize humans from their gait. Two different image features have been considered: the width of the outer contour of the binarized silhouette of the walking person and the entire binary silhouette itself. To obtain the observation vector from the image features, we employ two different methods. In the first method, referred to as the indirect approach, the high-dimensional image feature is transformed to a lower dimensional space by generating what we call the frame to exemplar (FED) distance. The FED vector captures both structural and dynamic traits of each individual. For compact and effective gait representation and recognition, the gait information in the FED vector sequences is captured in a hidden Markov model (HMM). In the second method, referred to as the direct approach, we work with the feature vector directly (as opposed to computing the FED) and train an HMM. We estimate the HMM parameters (specifically the observation probability) based on the distance between the exemplars and the image features. In this way, we avoid learning high-dimensional probability density functions. The statistical nature of the HMM lends overall robustness to representation and recognition. The performance of the methods is illustrated using several databases.[21]

Mobile ID for law enforcement applications

Instant identification with biometric technology is another program designed to make sure everyone is under his thumb. Currently there are 26 companies in America that are providing instant identification technology to the civilian sector, to police and the military.[22]

These biometric technology companies have field equipment that can run fingerprint, facial and iris scans and even DBA samples within minutes. One of those companies, L-1 Identity Solutions, "provides a full range of finger/palm, face, iris, and multi-biometric products for government-sponsored civilian identification management programs and criminal identification management procedures managed by law enforcement and military agencies.

"With a global network of partners such as leading system integrators, defense prime contractors and OEMs, L-1 Identity Solutions serves a broad range of markets including federal, state and local government, law enforcement, financial services, border management and travel."[23]

This is what L-1 I.S. says about its products:

L-1's portable, hand-held mobile identification devices allow officers in the field to get accurate information about their suspects' identity immediately, instead of going to the booking station, where waiting time for results could be anywhere from three hours to three days. The products support multiple biometrics, enabling officers to verify an identity via a suspect's finger, face or iris pattern. The Mobile ID products help:

Save valuable time and improve the productivity of officers in the field by eliminating unnecessary trips to the police station.

Reduce the chance of incorrectly releasing a dangerous criminal, thereby increasing public safety.

Prevent false arrest and avert having an innocent individual endure the inconvenience and time loss associated with false arrest.

Officers to make more identifications based on multiple biometric recognitions. Leveraging more biometric data sources – finger, face and iris – means more hits that are more accurate.[24]

It is only a matter of time before police officers will make random checks of identification. They will randomly pull over drivers and check the ID of everyone in the vehicle. They will also check the ID of pedestrians.

The Nazis said, "Papers, please." Big Brother minions in America will command, "ID, now." Please will not be in their vocabulary.

The goal of Big Brother is to collect as much personal data as possible on the masses. In time police will routinely stop people for no reason just to get biometric data from them.

If you still believe that America is a free country where everyone can live their life the way they want to without being told how to live, what to say, what to think, what to like and what to dislike go back to page 13 and read the Introduction carefully. America was the fifth worse tyrannical nation in the world in 2010.

Biometrics for national security (NSPD 59/HSPD 24)

Another Big Brother police state measure that came from the Bush administration, with virtually no press coverage, was NSPD 59 (HSPD

24) entitled **Biometrics for Identification and Screening to Enhance National Security**.

NSPD 59 was issued on June 5, 2008, four days prior to the publication of Rep. Dennis Kucinich's Articles of Impeachment of President George W. Bush by the House of Representatives. It became "law" with no public debate or congressional approval. This presidential directive goes far beyond the issue of biometric identification recommending the collection and storage of "associated biographic" information (information on the private lives of US citizens, in minute detail, all of which will be "accomplished within the law"):

> The contextual data that accompanies biometric data includes information on date and place of birth, citizenship, current address and address history, current employment and employment history, current phone numbers and phone number history, use of government services and tax filings. Other contextual data may include bank account and credit card histories, plus criminal database records on a local, state and federal level. The database also could include legal judgments or other public records documenting involvement in legal disputes, child custody records and marriage or divorce records."

It also calls for the integration of various data banks as well as inter-agency cooperation in the sharing of information, with a view to eventually centralizing the information on American citizens. In a carefully worded text, NSPD 59 "establishes a framework" to enable the Federal government and its various police and intelligence agencies to: "use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."

The directive recommends: "actions and associated timelines for enhancing the existing terrorist-oriented identification and screening processes by expanding the use of biometrics."[25]

The Bush administration took full advantage of the 911 attacks to pass and implement myriad Big Brother laws. The rush toward a total dictatorship by the Bush administration has been excelerated by the Obama administration. Total dictatorship is inevitable unless the American people stand up and say, "NO!"

KSTs
(NSPD 59)

The stated intent of NSPD 59 is to protect America from terrorists, but in fact the terms of reference include any person who is deemed to pose a threat to the Homeland. The government requires the ability:

> to positively identify those individuals who may do harm to Americans and the Nation . . . Since September 11, 2001, agencies have made considerable progress in securing the Nation through the integration, maintenance, and sharing of information used to identify persons who may pose a threat to national security.

The Directive is not limited to KSTs, which in Homeland Security jargon stands for "Known and Suspected Terrorists":

> The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security.
>
> The executive branch recognizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient. For example, while existing name-based screening procedures are beneficial, application of biometric technologies, where appropriate, improve the executive branch's ability to identify and screen for persons who may pose a national security threat. To be most effective, national security identification and screening systems will require timely access to the most accurate and most complete biometric, biographic, and related data that are, or can be, made available throughout the executive branch."[26]

Radical groups & disgruntled employees

NSPD 59 calls for extending the definition of terrorists to include other categories of individuals "who **may** pose a threat to national security."

In this regard, it is worth noting that in the 2005 TOPOFF (Top officials) anti-terror drills, two other categories of individuals were identified as potential threats: "Radical groups" and "disgruntled

employees," suggesting than any form of dissent directed against the federal government will be categorized as a threat to America.[26]

Universal Adversary

In a previous 2004 report of the Homeland Security Council, entitled "Planning Scenarios," the enemy was referred to as the Universal Adversary (UA).

The Universal Adversary was identified in the scenarios as an abstract entity used for the purposes of simulation. Yet upon more careful examination, this UA was by no means illusory. It included the following categories of potential "conspirators": "foreign [Islamic] terrorists," "domestic radical groups," [antiwar and civil rights groups] "state sponsored adversaries" ["rogue states," "unstable nations"] and "disgruntled employees" [labor and union activists].[27]

DNA collection

CODIS

The **Combined DNA Index System** (**CODIS**) is a DNA database funded by the United States Federal Bureau of Investigation (FBI). It is a computer system that stores DNA profiles created by federal, state, and local crime laboratories in the United States, with the ability to search the database to assist in the identification of suspects in crimes.[28]

The Newborn Screening Saves Lives Act of 2007

Government bureaucrats want to create a DNA database that will eventually have a DNA sample from every man, woman and child in America. They have already started to build a DNA data base.

In April of 2008, then President Bush signed into law S. 1858, which allows the federal government to screen the DNA of all newborn babies in America. This was to be implemented within 6 months, meaning that this measure is now being carried out. Congressman Ron Paul states that this bill is the first step towards the establishment of a national DNA database. S. 1858, known as "The Newborn Screening Saves Lives Act of 2007," is justified as a "national contingency plan" in that it represents preparation for any sort of public health emergency.[29]

Government bureaucrats want to create a DNA database that will eventually have a DNA sample from every man, woman and child in America.

Feds to collect DNA

The federal government began to collect DNA samples from everyone arrested by a federal law enforcement agency.

Using authority granted by Congress through two different laws passed in 2005 and 2006, the government also plans to collect DNA samples from foreigners who are detained, whether they have been charged or not. The DNA would be collected through a cheek swab, said Justice Department spokesman Erik Ablin. That would be a departure from current practice, which limits DNA collection to **convicted felons**.

Expansion of the DNA database, known as CODIS, raises civil liberties questions about the potential for misuse of such personal information, such as family ties and genetic conditions. Justice officials estimate the new collecting requirements would add DNA from an additional 1.2 million people to the database each year.

A Chicago study in 2005 found that 53 murders and rapes could have been prevented if a DNA sample had been collected upon arrest. "Many innocent lives could have been saved had the government began this kind of DNA sampling in the 1990s when the technology to do so first became available," said Sen. Jon Kyl (R-Az).

Thirteen states have laws similar to the federal one: Alaska, Arizona, California, Kansas, Louisiana, Maryland, Minnesota, New Mexico, North Dakota, South Dakota, Tennessee, Texas and Virginia.[30]

Big Brother wants your DNA and he will not stop until he gets it or you are dead. Do not let him get it for as long as you can. Some will deny him their DNA to the point of death.

DNA taken upon arrest not conviction

The government plans to begin collecting DNA samples from anyone arrested by a federal law enforcement agency – a move intended to prevent violent crime, but which also is raising concerns about the privacy of innocent people. Using authority granted by Congress, the government also plans to collect DNA samples from foreigners who are detained, whether they have been charged or not.

Justice Department spokesman Erik Ablin said the DNA would be collected through a cheek swab. This would be a departure from current practice, which limits DNA collection to convicted felons.[31]

"The F.B.I., with a DNA database of 6.7 million profiles, expects to accelerate its growth rate from 80,000 new entries a year to 1.2 million by 2012 – a 17-fold increase. F.B.I. officials say they expect DNA processing backlogs – which now stand at more than 500,000 cases – to increase."[32]

The goal is to get a DNA sample from everyone in America and the planet. It will only be a matter of time before the bureaucrats get their wish.

Police draw blood

A select cadre of officers in Idaho and Texas received training in 2009 to draw blood from those suspected of drunken driving. The federal program's aim is to determine if blood drawn by police officers can be an effective tool against drunk drivers. If the results seem promising after a year or two, the National Highway Traffic Safety Administration will encourage police nationwide to undergo similar training.

"Officers cannot hold down a suspect and force them to breath into a tube but they can forcefully take blood – a practice that's been upheld by Idaho's Supreme Court and the U.S. Supreme Court," said Ada County, Idaho, Deputy Prosecutor Christine Starr. (It is much easier for police to force an uncooperative suspect to breath into a tube than to draw blood. A suspect could bleed to death if he resisted and the officer cut a vein or artery.)

The nation's highest court ruled in 1966 that police could have blood tests forcibly done on a drunk driving suspect without a warrant, as long as the draw was based on a reasonable suspicion that a suspect was intoxicated, that it was done after an arrest and carried out in a **medically approved manner**.

"I would imagine that a lot of people would be wary of having their blood drawn by an officer on the hood of their police vehicle," said Steve Oberman, chair of the National Association of Criminal Defense Lawyers' DUI Committee.

Once the trained officers are back on patrol, they will draw blood of any suspected drunk driver who refuses a breath test. They will use

force if they need to, such as getting help from another officer to pin down a suspect and potentially strap them down.

This is beyond incredible! This makes the Nazis look like girl scouts. This bizarre practice started in 1995 in Arizona.

This weird Big Brother scheme has numerous problems. Vials can be mixed up, preservative levels in the tubes used to collect the blood can be off, or the blood can be stored improperly, causing it to ferment and boosting the alcohol content. Lawsuits should eventually put an end to this insane practice.

If this scheme becomes commonplace around the country what will keep Big Brother from drawing blood in the field from anyone who is detained by police? If Big Brother wants a DNA sample from everyone, one way of getting a sample from those who do not voluntarily give it is to have police officers randomly demand a blood sample from anyone they stop. Instead of demanding identification they will also demand blood or saliva from a cheek swab.[33]

HIV testing at the DMV

One Department of Motor Vehicles office in Washington, D.C. began a program in which motorists could be tested for HIV when they applied for a driver's license or to renew one.

Participants in this first-of-its-kind will receive up to $15 to help defray their DMV costs. "We wanted to have a broad audience and a captive audience. You're captive at the DMV," said Angela Fulwood Wood, chief operations officer of the Family and Medical Counseling Service. "We're **normalizing people's thoughts** of testing. You can do organ donation at the DMV. You can do voter registration at the DMV. If people don't want to do it, we can at least talk to them."

The city Health Department is supplying HIV testing kits and educational materials, and the DMV is contributing office space. Family and Medical Counseling Service received $250,000 in funding from Gilead Sciences, a Foster City, California, biopharmaceutical company, to help cover staff costs and the $15 money orders.

Gilead spokeswoman Cara Miller said in an e-mail that the project is in keeping with the company's efforts to "**normalize**" testing in "traditional and non-traditional settings."[34]

This may be a program designed to help people, but it may also be a way to get a DNA sample from people. Big Brother is very sneaky and devious.

New portable DNA screener

Homeland Security plans to begin testing a DNA analyzer in the summer of 2011 that is small enough to be portable and fast enough to return results in less than an hour.

The analyzer, known as a rapid DNA screener, is about the size of a laser printer. Initially will be used to determine kinship among refugees and asylum seekers. It also could help establish whether foreigners giving children up for adoption are their parents or other relatives, and help combat child smuggling and human trafficking. Eventually, the analyzer also could be used to positively identify criminals, illegal immigrants, missing persons and mass casualty victims, he said.

Using a process called digital micro-fluidics, the analyzer processes a DNA sample and provides results in less than an hour for under $100 per sample as compared to the days or weeks and $500 per sample to get results when it is tested in a laboratory.

As with other DNA tests, the process begins with a sample collected on a swab, typically from inside the mouth. The sample is placed in a disposable cartridge, and the analyzer does the rest of the work.

"We're not about advancing the technology so much as integrating and automating it into a fieldable device," said Christopher Miles, biometrics program manager in the DHS Office of Science and Technology.

Boston-based NetBio, which developed the rapid DNA analyzer for DHS, described it as a "game-changing technology" platform that "consists of instruments, biochips and analytical software." It eliminates the need for a trained technician and special operating site. The analyzer was designed for Homeland Security, the military, intelligence and police agencies.

The machines are expected to cost about $275,000 apiece. "That sounds like a lot of money, but compare that to a laboratory full of equipment that would cost millions of dollars and a building that would cost tens of millions of dollars." After the rapid analyzers are in production, he added, the cost is likely to come down.[35]

Ten years from now the cost of these machines could drop to a few thousand dollars a piece. The speed of identifying a person will also drop to just a few minutes. When the price drops low enough police departments will buy them to put in patrol cars so a person's identity can be verified within a few minutes. Eventually stores and all government offices will have them to make a positive ID of everyone apply for benefits or seeking government services.

As noted previously, Big Brother will routinely gather biometric data from the masses through police officers. He will also have his minion officers collect DNA from people with no justifiable reason. A DNA sample is the holy grail of biometric data.

Big Brother wants your DNA and he will think up any scheme to get it. Do not fall for his scams. Keep your DNA to yourself and tell Big Brother he cannot have it.

Biometrics Identity Management Agency

On March 23, 2010, the Biometrics Task Force (created in 2000) was redesignated the Biometrics Identity Management Agency (BIMA).

"The Biometrics Identity Management Agency leads Department of Defense activities to prioritize, integrate, and synchronize biometrics technologies and capabilities and to manage the Department of Defense's authoritative biometrics database to support the National Security Strategy," according to the March 23 order issued by Army Secretary John M. McHugh (www.fas.org/irp/doddir/army/bima.pdf).

Dr. Thomas Killion, the former Chief Scientist of the U.S. Army who served as Science Advisor to the Director of Joint IED Defeat Organization, became Director of BIMA on October 26, 2010.[36]

Fingerprinting

History of fingerprinting

Fingerprinting for identification is an old Big Brother technology that was first used in Babylon in 1750 B.C. In 300 A.D. the Chinese used handprints for evidence in trials and by 650 A.D. they knew fingerprints could be used to identify people. By 1300 A.D. they used fingerprints for identification. The British used them in India for identification, and in 1891 an Argentine police chief created the first modern fingerprint file. Scotland Yard created the first fingerprint bureau in 1901, and in 1906 the New York Police Department introduces fingerprinting to America.

Today virtually every nation on Earth has programs designed to get the prints of everyone, including children. Big Brother is fingerprint crazy.

Fingerprinting real estate agents

The Senate housing bill of 2008 contains a provision to create a new national fingerprint registry. It covers just about everyone involved in the mortgage business, including lenders, "loan originators," and some "real estate agents."[37]

Real estate certainly has its risks and fraud is a growing problem, but now there's a new law that's supposed to protect buyers. As CBS 2's Mike Puccinelli reports the new law will also place an unusual burden on the seller.

Fingerprinting is something we often associate with crime. So the fact that Cook County home sellers will soon have to provide a thumb print left some people shocked. The new law, set to go into effect June 1, 2009, will force anyone selling property in Cook County to provide a thumbprint from their right hand.[38]

Auto rentals

James Glave said he learned about the mandatory thumbprinting when he sought to rent a car from Dollar Rent A Car. He noticed a display featuring a drawing of a big thumb, with the words "Thumbs Up!" printed on it. Glave explained that thumbprints were being collected from customers as part of an effort to reduce fraud and theft. When he did not comply, the employee refused to rent him a car.[39]

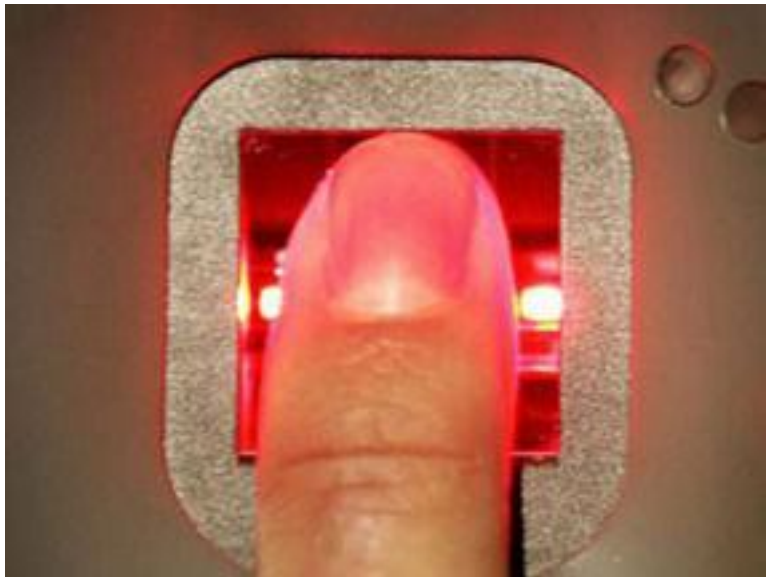
When Big Brother demands a thumbprint, fingerprint or any biometric identification tell him "NO!" Go elsewhere to buy a product or service. The way to slow Big Brother down is to stop buying his junk and worthless services. If you cannot purchase an item or a service without giving him biometric information do without it.

Thumbprint at checkout stand

A pet store in Herndon, Va., accepts cash, credit cards, checks or your thumbprint. Customers at **Fox Mill Pets** can pay for their goods and pets by placing a thumb on a fingerprint scanner at the register.

The scanner which is connected to a computer network analyzes the print and matches the print to the customer. The customer's checking account is then debited the amount of the purchase.

Biometric devices such as fingerprint readers, retinal scanners and facial recognition systems are often part of high-tech security, but until



This technology will replace cash, checks and credit cards.

2002, biometrics has been considered too expensive and cumbersome for everyday use.

Fox Mill Pets, Eleven **Food 4 Less** stores in the Midwest, three **Kroger** grocery stores in Texas and **Duthler Family Foods** in Grand Rapids, Michigan are trying fingerprint scanners along with other shops. **BioPay** (www.biopay.com), which has the nation's largest commercial electronic **fingerprint database**, is the leader in this industry.[40]

"It improves productivity, reduces operating costs, improves cash flow and lowers fraud," said Ron Smith, CEO of **Biometric Access**, which makes fingerprint systems similar to the one at Fox Mill Pets. "It puts the 'express' in 'express lane.'" **Pay By Touch** is another company making a similar product.

For most systems customers must sign up which takes about five minutes. They must provide their name, phone number and checking account or credit card information. Two index fingers are scanned and an electronic photo is taken of the customer. The next time customers buy something the computer compares their print with ones in the database to find a match.

A major problem with this system is security. The customer's biometric information is stored in the computer system in the store and at the office of the company that supplies the scanners. Every customer's negative check-cashing information is stored in a central

database and shared between all merchants using the BioPay system. A hacker or employee can steal this information. “All it takes is one good breach,” said Will Doherty of online advocacy group Electronic Frontier Foundation.

Southern California grocery chain **Cardenas Market** lost $500,000 a year on check-cashing fraud, but since they started using biometric fingerprint scanners in its nine stores fraud has dropped to one-percent said general manager Steve Vallance. “Biometrics is one way to really identify the customer you’re dealing with,” he says.[41]

Biometric identification is an excellent way to eliminate fraud. But there is a better way to stop fraud and not infringe on the privacy of people. The perfect solution is cash. It may cause criminals to engage in more mugging and theft of purses and wallets, but it is nothing compared to credit card and electronic fraud.

Mexico to fingerprint buyers of cell phones

Mexico will start a national register of mobile phone users that will include fingerprinting all customers in an effort to catch criminals who use the devices to extort money and negotiate kidnapping ransoms.

Under a new due to be in force in April of 2009, mobile phone companies will have a year to build up a database of their clients, complete with fingerprints.

Hundreds of people are kidnapped in Mexico every year and the number of victims is rising sharply as drug gangs seek new income. Politicians who pushed the bill through Congress say there are around 700 criminal bands in Mexico, some of them operating from prison cells that use cell phones to extract extortion and kidnap ransom payments.

Most of Mexico’s 80 million mobile phones are prepaid handsets with a given number of minutes of use that can be bought in stores without any identification. The phones can have more minutes added through purchases from vendors on street corners.

The plan also requires operators to store all cell phone information such as call logs, text and voice messages, for one year. Information on users and calls will remain private and only available with court approval to track down criminals.

Unregulated vendors sell cell phones and chips for cash from street side stands. It is unclear how such vendors would be made to comply with the new law.[42]

Tennessee traffic violaters could get fingerprinted

Motorists stopped for traffic violations in Tennessee could be fingerprinted if state lawmakers approve a bill pending in the legislature.

Currently, when drivers are cited during traffic stops, police officers ask for the driver's signature on the ticket, but the proposed bill would allow police departments to the choice of collecting a signature or a fingerprint, or collecting a signature and a fingerprint.

Supporters say collecting fingerprints would save money and help police determine whether the driver is wanted for a criminal offense, but opponents worry that it allows the government to tread on individual privacy rights.[43]

Houston teachers next in line to be fingerprinted

Senate Bill 9, approved in September 2007, requires all certified staff members and substitute teachers of the Houston Independent School District to be fingerprinted by September 1, 2011. New hires have been required to do this since January 1, 2008.

The process is pretty rigid. After the Texas Education Agency notifies the district, they will have 80 days to fingerprint eligible employees. The fingerprinting is done through a state-selected vendor, and prints must be deemed acceptable by the FBI and Department of Public Safety by the district's March 5 deadline.

Any employee who does not meet the standard by the deadline will have their certificate deactivated. If the district discovers any felonies, the employee will be dismissed.[44]

Vending Machines Take Finger Scans Instead of Cash

Biometric scanners are popping up everywhere, and now Hitachi has debuted the first vending machine that will accept a finger scan instead of cash or coins. By linking the scan to a credit card account, customers can simply place their finger in the machine and make a purchase.

The biometric sensor in Hitachi's new vending machine uses light to scan and read the number and orientation of veins in your finger tip without directly touching a sensor. Hitachi has not decided if it will market the machine.[45]

UK police to use mobile fingerprint scanners

All United Kingdom police forces will be issued mobile fingerprint scanners amid plans to carry out random identity checks on people in the street.

The hand-held devices will enable every officer on the ground to receive instant images of suspects as part of a scheme codenamed Project Midas. No bigger than a BlackBerry smartphone, the technology will be widely distributed to every force in the UK by spring of 2011.

The Home Office is understood to have already allocated £50 million for 10,000 of the mobile devices by September. A prototype machine has already been used during a series of tests carried out by motorway patrols.

Large public occasions, sporting events, festivals and political conferences could be targeted as well as the 2012 London Olympics.[46]

Biometric ID in Scottish schools

Dozens of Scottish schools have introduced "intrusive" biometric systems, such as fingerprinting, to identify pupils as young as four. New figures show 68 schools are now using technology to manage meals, control library books and even allow access to toilets.[47]

UK school prints children without consent

Capital City Academy in Brent, north London, caused an uproar after taking children's fingerprints without permission from their parents.

Pupils were forced to be fingerprinted so they could use touch screens in the canteen to have money deducted from their account. It also introduced an opt-out for parents uncomfortable with the technology, allowing pupils to enter a four-digit pin code instead of scanning their print.

The revelation comes as teachers today warned schools are routinely taking children's fingerprints without permission from their parents. As many as 3,500 schools in the UK take biometric data from pupils to speed up basic administration such as buying canteen lunches or borrowing library books. A 2007 survey by the Liberal Democrats found that out of 285 schools using fingerprint scanners, only 48 had first sought parental consent.

Hank Roberts of the Association of the Teachers and Lecturers said civil liberties were being eroded. “There has been a severe diminution of civil liberties and freedoms in this country and we face the danger of more and worse to come. It’s outrageous that children’s fingerprints can be taken without parents’ consent.”

“Should we allow Big Brother in our schools?” asked Azra Haque, a teacher from Brent. “Today’s children are in general much more closely monitored than previous generations. We really do need a strong and explicit law in this regard.”[48]

Parents to be fingerprinted in the UK

Up to 50 nurseries and playgroups in the United Kingdom have already signed up for a new security measure that requires parents to be fingerprinted.

Up to 50 nurseries and playgroups have signed up for the new security measures, thought to be the first time parents have been targetted in this way. The new entry system requires people who collect their children to place their finger on a scanner, to make sure that only nominated individuals can get through secure entrances.

Kidsunlimited, the nursery chain, will be rolling out the new technology to its 50 playgroups. Honeycomb Solutions, the security firm behind the technology, says it is an effective way to monitor who is on their premises.

George Bathurst, Managing Director of Honeycomb Solutions said: “This cutting edge system will revolutionise the way we keep our children safe by ensuring that only authorised people can get into the classroom. Even when you have authorisation staff will know who you are, and when arrived. This can be monitored centrally, providing an additional layer of security. We predict that within the next five years this system will become common place across the country.”[49]

Nine industries that know your every move

The government agency that gathers the most personal information on millions of Americans is the Federal Bureau of Investigation. It keeps a database of over 90 million fingerprints, which can be accessed by other law enforcement agencies. It also has an extensive DNA database. The bureau’s ability to collect information expanded following the terrorist attacks of September 11, 2001. It now tracks a

large portion of mail, cell phone traffic and Internet activity of people it deems suspicious.

Thanks to advances in technology thousands of corporations track and record your every move. Although they share some of their information about you with government agencies and other corporations, there are numerous security breaches where sensitive information about their customers is stolen.

The following sectors of commercial industry have a great deal of information about you:

1. Credit rating corporations

The three credit bureaus – Equifax (EFX), Experian (EXPGY), and TransUnion – know not only your credit history, but also have the data to project your credit future. Each has files on over 200 million people. The companies collect a history of all credit use by an individual, including payment of bills, mortgages, and credit cards.

2. Cell phone service providers

Cell phone companies have come to possess a wealth of information about their customers. Covering over 90% of the American population, cell phone providers can tell who you call, when you call, how often you call certain people and what you say in your text messages. With GPS, they also now know where you are whenever you have your phone. As smartphones become the equivalent of miniature computers, cellular companies can also track personal behavior, such as use of multimedia and wireless e-commerce transactions.

3. Social media companies

Facebook has amassed an enormous amount of user information. It knows who your friends are, what you like, and what photos you are in. It also tracks which profiles you view, who you communicate with most often, companies and causes you support, your personal calendar, and personal information about your friends and family. This ominous corporation can also access the information you have deleted, including photos and status updates, from their servers.

4. Credit card companies

There are currently 610 million credit cards owned by U.S. consumers. In an economy dominated by credit, the amount of power held by credit card companies, such as Visa, MasterCard and American Express, should not be surprising. They know their customers' credit scores, credit histories, what they buy, when they buy, and when they are likely to default on their payments.

5. Search engines

Every search you perform on Google goes into its database, which it uses to keep a profile of your habits and interests. The search engine also keeps track of which links you click on during your search and which advertisers you visit. Google uses your interest profile and search history to place targeted ads in your browser. Perhaps most disturbingly, Google uses its Gmail service to monitor the content of your email in order to place targeted advertising in your email account. Google even keeps records of account and credit card information for everyone who uses their "Checkout" service, tracks which videos people watch on YouTube, where people are planning to visit, and what they plan to do there. Google's location-based map systems also allow the search company to know where people are in real time through the use of smartphones and other GPS-enabled devices.

6. Retail chains

Walmart uses data-mining services to collect and store information for all its customers in a central location. This allows it to determine the purchasing behavior of people who shop in its stores or on its website. It also optimizes inventory distribution by determining which products people are most likely to buy in the future. In August, Walmart began installing Radio Frequency Identification Devices (RFID) in their underwear and jeans, which lets them track items and customers around the store. This means they are able to determine how much time someone who buys a specific pair of pants spends in each aisle. Walmart plans to use this data to reorganize displays and further control inventory. The retail giant also sells this information to thousands of other businesses, who use consumer profiles for advertising and demographic research.

7. Casinos

Casinos like the Wynn Resorts are increasingly using "loyalty cards" to monitor the behavior of their patrons. The Wynn "red" cards are used in place of tokens, and allow the casino to keep track of which machines and tables each gambler visits on a regular basis, the path they take during their visits (using RFID chips), and even how often and how much they are willing to lose before giving up. When a slot machine in Wynn detects a gambler is close to his breaking point, it will issue a small payout in order to keep him spending money.

8. Banks

Large banks, such as Bank of America, Chase and Citibank, have access to customer account information, which includes savings, employer payroll deposits, and the time and date of ATM and teller visits. They track transfers made by account holders to third parties. A bank also knows your income, your salary, and your balance, moment-by-moment. Perhaps among the most confidential data a bank keeps is how often people move money in and out of accounts. Banks know how much you save each month, and often exactly how those savings are invested. Banks use this information to assess the risk of giving you a mortgage or loan, and they are legally allowed to use data-mining companies to check your website activity.

9. Life insurance companies

About 140 million households have life insurance. In order to apply for it, applicants generally must disclose their health history. This includes incidence of heart disease, height, weight, smoking habits, and often includes full records from your doctors. Perhaps more invasive, life insurers seek disclosure of hospitalization for mental illness, use of illegal drugs, and whether or not you have had to file for bankruptcy. Insurance companies use a national prescription database to determine whether or not you have ever been prescribed medication. And certain high-risk professions and hobbies usually have to be disclosed.[50]

Conclusion

Within 10 years virtually all forms of identification will incorporate biometrics. Driver's licenses will have biometric identification markers as mandated by law and most credit cards will also.

Most retail outlets will require some form of biometric identification to get a rewards card or to make purchases. Checks and credit cards will eventually be phased out by most major retail outlets. Cash will also disappear and people who purchase goods with cash will be identified and placed on a watch list as a suspected terrorist.

Yet even though the Big Brother net will get bigger and draw most people in the best way to proceed is to NOT opt into the program. Keep buying with cash and do NOT give the state, bank or any company biometric information. Refuse all DNA, facial, retinal and fingerprint scans. Life will get harder for true Patriots but we must resist and work together.

Notes

1. Steinmetz, Katy. "Ready for Your Biometric Social Security Card?" Time. 3.29.2010. www.time.com/time/nation/article/0,8599,1974927,00.html?xid=feed-yahoo-full-nation-related.

2. Saenz, Aaron. "India Launches Universal ID System with Biometrics." 9.13.2010. http://singularityhub.com/2010/09/13/india-launches-universal-id-system-with-biometrics.

3. http://en.wikipedia.org/wiki/Resident_Identity_Card.

4. Richtel, Matt. "In Texas, 28,000 Students Test an Electronic Eye." TexasISD.com. 11.17.2004. www.texasisd.com/artman/exec/view.cgi/25/22495.

5. "Homeland Security to test iris scanners." USA Today. 9.13.2010 www.usatoday.com/tech/news/surveillance/2010-09-13-1Airis13_ST_N.htm.

6. Saenz, Aaron. "Iris Scanning Set To Secure City in Mexico, Then the World." 9.26.2010. http://singularityhub.com/2010/09/26/iris-scanning-set-to-secure-city-in-mexico-then-the-world-video.

7. Howard, Zach. "Law enforcement to begin iPhone iris scans amid privacy concerns." Reuters, 7.20.2011. www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720?feedType=SS&feedName=domesticNewsrpc=22&sp=true.

8. "Log-in to Facebook with an iris scan: Eye-scanner for your PC set to go on the market in months." Daily Mail. 5.11.2011. www.dailymail.co.uk/sciencetech/ article-1385959/Under-look-key-PC-iris-scanner-security-device-set-market-months. html.

8b. Hastings, Rob. "Iris-scanning registration booths scaled back." 11.15.2011. www.independent.co.uk/news/uk/home-news/irisscanning-registratio n-booths-scaled-back-6262597.html.

9. Retinography: How Retinal Scanning Works. www.discoveriesinmedicine.com/Ra-Thy/Retino graphy.html.

10. “Eye Prints.” TIME Magazine. 12.16.1935. www.time.com/time/printout/0,8816,755453,00.html.

11. Hill, Robert. “Retina Identification.” Msu.Edu. www.cse.msu.edu/~cse891/Sect601/textbook/6.pdf.

12. http://en.wikipedia.org/wiki/Facial_recognition_system.

13. http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm.

14. Herald Sun. “Nightclub goes for face-scanning security.” 4.23.2009. www.news.com.au/heraldsun/story/0,21985,25373233-2862,00.html & http://pursuito.wordpress.com/2009/04/26/nightclub-goes-for-face-scanning-security & www.youtube.com/watch?v=c8NGjcMnXmw.

15. Yapp, Robin. “Brazilian police to use ‘Robocop-style’ glasses at World Cup.” 4.12.2011. www.telegraph.co.uk/news/worldnews/southamerica/brazil/8446088/Brazilian-police-to-use-Robocop-style-glasses-at-World-Cup.html.

16. Steve Cain, Lonnie Smrkovski and Mindy Wilson. http://expertpages.com/news/voiceprint_identif ication.htm.

17. Finn, Peter. “Report: Top al-Qaeda figure killed Pearl.” Washington Post. 1.20.2011. www.washingtonpost.com/wp-dyn/content/article/2011/01/19/AR2011011907114.html.

18. Blackburn, Bradley. 1.20.2011. “Report Says Justice Not Served in Murder of Daniel Pearl, Wall Street Journal Reporter. ABC News. pp. 1–2. http://abcnews.go.com/US/report-justice-served-murder-daniel-pearl/story?id=12721909.

19. Cratty, Carol. “Photos of hands backed up Pearl slaying confession, report finds.” CNN. 1.20.2011. www.cnn.com/2011/WORLD/asiapcf/01/20/pakistan.daniel.pearl.execution.

20. Ackerman, Spencer. “Qaeda Killer’s Veins Implicate Him In Journo’s Murder.” Wired. 1.20.2011. www.wired.com/dangerroom/2011/01/qaeda-killers-veins-implicate-him-in-journos-murder.

21. Kale, Amit, Sundaresan, Aravind, Rajagopalan, A.N., Cuntoor, Naresh P., Roy-chowdhury, Amit K., Krüger, Volker. “Identification of humans using gait. 2004. www.cfar.umd.edu/~cuntoor/01323098.pdf & www.cfar.umd.edu/~kale/myproposal.pdf & www.ee.ucr.edu/~amitrc/iptrans_gait.pdf & www.metaverselab.org/pub/paper2/hmmjrnl.pdf.

22. www.thomasnet.com/products/identification-systems-biometric-95992699-1.html.

23. www.l1id.com/pages/17-biometrics.

24. www.l1id.com/pages/46-mobile-id-for-law-enforcement.

25. http://en.wikipedia.org/wiki/NSPD-51.

26. www.fas.org/irp/offdocs/nspd/nspd-59.html.

27. Chossudovsky, Michel. “‘Big Brother’ Presidential directive: ‘Biometrics for Identification and Screening to Enhance National Security’” Global Research. 6.13.2008. www.globalresearch.ca/index.php?context=va&aid=9296.

28. http://en.wikipedia.org/wiki/CODIS.

29. “The Bill Nobody Noticed: National DNA Databank.” GovTrack.us. S. 1858 – 110 Congress (2007): Newborn Screening Saves Lives Act of 2007, GovTrack.us (database of federal legislation) www.govtrack.us/congress/bill.xpd?bill=s110-1858.

30. Sullivan, Eileen. “Feds to collect DNA from every peson they arrest.” AP. Yahoo News. 4.16.2008. http://news.yahoo.com/s/ap/20080416/ap_on_go_ca_st_pe/

dna_collection. & State Laws on DNA Data Banks: www.ncsl.org/programs/cj/dnadatabanks.htm & www.dnaresource.com/documents/2008DNAExpansionLegislation.pdf.

31. Sullivan, Eileen. "Feds to collect DNA from every person they arrest." Yahoo News. 4.16.2008. Associated Press. http://news.yahoo.com/s/ap/20080416/ap_on_go_ca_st_pe/dna_col lection.

32. New York Times. "F.B.I. and States Vastly Expand DNA Databases." www.nytimes.com /2009/04/19/us/19DNA.html?_r=2.

33. Boone, Rebecca. "Police say syringes will help stop drunk driving. 9.15.2009. www.policeone.com/patrol-issues/articles/1883923-Police-say-syringes-will-help-stop-drunk-driving.

34. Stewart, Nikita. "D.C. brings HIV testing to the crowd at the DMV." 9.30.2010. www.washington post.com/wp-dyn/content/article/2010/09/30/AR2010093003463_pf.html.

35. Matthews, William. "New portable DNA screener to debut this summer." NextGov.com. 2.24.2011. www.nextgov.com/nextgov/ng_20110224_1299.php?oref=topnews.

36. Aftergood, Steve. "A U.S. Biometrics Agency." Secrecy News. 3.29.2010. www.fas.org/blog/secrecy/2010/03/biometrics_agency.html & www.biometrics.dod. mil.

37. McCullagh, Declan. "Housing bailout bill creates national fingerprint registry." Cnet. 3.23.2008. http://news.cnet.com/8301-13578_3-9951420-38.html.

38. Puccinelli, Mike. "Giving The Fingerprint: Home Law Raises Concern." CBS. 3.14. 2009. http://cbs2chicago.com/local/Mike.Puccinelli.fingerprint.2.957819.html.

39. Scheeres, Julia. **"**No Thumbprint, No Rental Car." Wired. 11.21.2001. www.wired.com/politics/security/news/2001/11/48552.

40. "BioPay Announces Check Guarantee Program for Grocers." 1.26.2002. www.prweb.com/releases/2002/01/prweb32495.htm.

41. Kessler, Michelle. "Thumbs pay at some stores." USA Today. 11.16.2003. www.usatoday.com/tech/news/techinnovations/2003-11-17-biometrics_x.htm.

42. "Mexico 'to fingerprint all mobile phone owners'" 2.09.2009. www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/mexico/4573514/Mexico-to-fingerprint-all-mobile-phone-users.html.

43. Young, Nicole. "Tennessee speeders could get fingerprinted." The Tennessean. 5.16.2009. www.tennessean.com/article/20090516/NEWS03/905160341/Tennessee+speeders+could+get+fingerprinted.

44. Houston Chronicle. "Houston teachers next in line to be fingerprinted." 11.06.2009. http://blogs.chron.com/schoolzone/2009/11/houston_teachers_next_in_line.html.

45. Saenz, Aaron. "Vending Machines Take Finger Scans Instead of Cash." 8.24.2009. http://singularityhub.com/2009/08/24/vending-machines-take-finger-scans-instead-of-cash.

46. Drake, Matthew. "Police to get mobile fingerprint scanners amid plans to hold random identity checks." Daily Mail. 10.27.2009. www.dailymail.co.uk/news/article-1080841/Police-mobile-fingerprint-scanners-amid-plans-hold-random-identity-checks.html.

47. "BIOMETRIC ID CHECK ON SCOTS SCHOOLCHILDREN AS YOUNG AS FOUR." 12.28.2010. www.express.co.uk/posts/view/219758/Biometric-ID-check-

on-Scots-schoolchildren-as-young-as-fourBiometric-ID-check-on-Scots-schoolchildren-as-young-as-four#ixzz19jJwUcix.

48. Clark, Laura. “Pupils ‘frogmarched by teachers to have fingerprints taken’ so they could eat in canteen.” 3.30.2010. www.dailymail.co.uk/news/article-1262087/Schools-taking-fingerprints-pupils-parent s-knowing.html.

49. Khan, Urmee. “Parents to be fingerprinted by nursery schools. 10.29.2008. www.telegraph.co.uk/news/uknews/3275246/Parents-to-be-fingerprinted-by-nursery-schools.html.

50. McIntyr, Douglas. “Nine industries that know your ever move.” Daily Finance, 9.24.2010. www. dailyfinance.com/story/credit/who-is-watching-you-nine-industries-that-know-your-every-move/19629445.