Physical Security

RS&RM

Contents

Chapter 1

Security

For other uses, see Security (disambiguation).

Security is the degree of resistance to, or protection from,

X-ray machines and metal detectors are used to control what is allowed to pass through an airport security perimeter.

Security spikes protect a gated community in the East End of London.

harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

Security checkpoint at the entrance to the Delta Air Lines corporate headquarters in Atlanta

As noted by the Institute for Security and Open Methodologies (ISECOM) in the OSSTMM 3, security provides "a form of protection where a separation is created between the assets and the threat." These separations are generically called "controls," and sometimes include changes to the asset or the threat.*[1]

1.1 Perceived security compared to real security

Perception of security may be poorly mapped to measureable objective security. For example, the fear of earthquakes has been reported to be more common than the fear of slipping on the bathroom floor although the latter kills many more people than the former.*[2] Similarly, the perceived effectiveness of security measures is sometimes different from the actual security provided by those measures. The presence of security protections may even be taken for security itself. For example, two computer security programs could be interfering with each other and even cancelling each other's effect, while the owner believes s/he is getting double the protection.

Security theater is a critical term for deployment of measures primarily aimed at raising subjective security without a genuine or commensurate concern for the effects of that measure on objective security. For example, some consider the screening of airline passengers based on static databases to have been Security Theater and Computer Assisted Passenger Prescreening System to have created a *decrease* in objective security.

Perception of security can increase objective security when it affects or deters malicious behavior, as with visual signs of security protections, such as video surveillance, alarm systems in a home, or an anti-theft system in a car such as a vehicle tracking system or warning sign. Since some intruders will decide not to attempt to break into such areas or vehicles, there can actually be less damage to windows in addition to protection of valuable objects inside. Without such advertisement, an intruder might, for example, approach a car, break the window, and then flee in response to an alarm being triggered. Either way, perhaps the car itself and the objects inside aren't stolen, but with *perceived security* even the windows of the car have a lower chance of being damaged.

1.2 Categorizing security

There is an immense literature on the analysis and categorization of security. Part of the reason for this is that, in most security systems, the "weakest link in the chain" is the most important. The situation is asymmetric since the 'defender' must cover all points of attack while the attacker need only identify a single weak point upon which to concentrate.

- Aviation security is a combination of material and human resources and measures intended to counter unlawful interference with aviation.
- Operations Security (OPSEC) is a complement to other "traditional" security measures that evaluates the organization from an adversarial perspective.*[3]

1.3 Security concepts

Certain concepts recur throughout different fields of security:

- Assurance - assurance is the level of guarantee that a security system will behave as expected
- Countermeasure - a countermeasure is a way to stop a threat from triggering a risk event
- Defense in depth - never rely on one single security measure alone
- Risk - a risk is a possible event which could cause a loss
- Threat - a threat is a method of triggering a risk event that is dangerous
- Vulnerability - a weakness in a target that can potentially be exploited by a security threat
- Exploit - a vulnerability that has been triggered by a threat - a risk of 1.0 (100%)

1.4 Security at home

Security at home is something applicable to all of us and involves the hardware in place on a property, and personal security practices. The hardware would be the doors, locks, alarm systems, lighting that is installed on your property. Personal security practices would be ensuring doors are locked, alarms activated, windows closed and many other routine tasks which act to prevent a burglary.

1.5 Security management in organizations

In the corporate world, various aspects of security are historically addressed separately - notably by distinct and often noncommunicating departments for IT security, physical security, and fraud prevention. Today there is a greater recognition of the interconnected nature of security requirements,*[4] an approach variously known as holistic security, "all hazards" management, and other terms.

Inciting factors in the convergence of security disciplines include the development of digital video surveillance technologies (see Professional video over IP) and the digitization and networking of physical control systems (see SCADA).*[5]*[6] Greater interdisciplinary cooperation is further evidenced by the February 2005 creation of the Alliance for Enterprise Security Risk Management, a joint venture including leading associations in security (ASIS), information security (ISSA, the Information Systems Security Association), and IT audit (ISACA, the Information Systems Audit and Control Association).

In 2007 the International Organisation for Standardization (ISO) released ISO 28000 - Security Management Systems for the supply chain. Although the title supply chain is included, this Standard specifies the requirements for a security management system, including those aspects critical to

security assurance for any organisation or enterprise wishing to manage the security of the organisation and its activities. ISO 28000 is the foremost risk based security system and is suitable for managing both public and private regulatory security, customs and industry based security schemes and requirements.

1.6 See also

- Safety

1.7 References

[1] "ISECOM - Open Source Security Testing Methodology Manual (OSSTMM)". Retrieved 20 September 2014.

[2] Bruce Schneier, *Beyond Fear: Thinking about Security in an Uncertain World*, Copernicus Books, pages 26-27

[3] OSPA. "The Operations Security Professional's Association- OPSEC Training, tools and Awareness" . Opsecprofessionals.org. Retrieved 2012-09-30.

[4] "Security in a Changing Landscape" . Dell.com. Retrieved 2012-03-27.

[5] Taming the Two-Headed Beast, CSOonline, September 2002

[6] Security 2.0, CSOonline, April 2005

1.8 External links

- Internet Identity Card Systems

Chapter 2

Physical security

Modern prisons are among some of the most physically secure facilities, with almost every area under tight access control and surveillance. Pictured here is the exterior of Shata Prison in Israel, which is secured through the use of high fences, razor wire, protective barriers, guard towers, and security lighting.

Canadian Embassy in Washington, D.C. showing planters being used as vehicle barriers to increase the standoff distance, and barriers and gates along the vehicle entrance

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).[*][1] Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques.

2.1 Overview

Physical security systems for protected facilities are generally intended to:[*][2][*][3][*][4]

- deter potential intruders (e.g. warning signs and perimeter markings);
- detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems); and
- trigger appropriate incident responses (e.g. by security guards and police).

It is up to security designers, architects and analysts to balance security controls against risks, taking into account the costs of specifying, developing, testing, implementing, using, managing, monitoring and maintaining the controls, along with broader issues such as aesthetics, human rights, health and safety, and societal norms or conventions. Physical access security measures that are appropriate for a high security prison or a military site may be inappropriate in an office, a home or a vehicle, although the principles are similar.

2.2 Elements and design

2.2.1 Deterrence methods

Main articles: Natural surveillance and Crime prevention through environmental design

The goal of *deterrence* methods is to convince potential attackers that a successful attack is unlikely due to strong defenses.

The initial layer of security for a campus, building, office, or other physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic: warning signs or window stickers, fences, vehicle barriers, vehicle height-restrictors, restricted access points, security lighting and trenches.*[5]*[6]*[7]*[8]

Physical barriers

Spikes atop a barrier wall act as a deterrent to people trying to climb over the wall

Physical barriers such as fences, walls, and vehicle barriers act as the outermost layer of security. They serve to prevent, or at least delay, attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult. Tall fencing, topped with barbed wire, razor wire or metal spikes are often emplaced on the perimeter of a property, generally with some type of signage that warns people not to attempt to enter. However, in some facilities imposing perimeter walls/fencing will not be possible (e.g. an urban office building that is directly adjacent to public sidewalks) or it may be aesthetically unacceptable (e.g. surrounding a shopping center with tall fences topped with razor wire); in this case, the outer security perimeter will be defined as the walls/windows/doors of the structure itself.*[9]

Natural surveillance

Another major form of deterrence that can be incorporated into the design of facilities is natural surveillance, whereby architects seek to build spaces that are more open and visible to security personnel and authorized users, so that intruders/attackers are unable to perform unauthorized activity without being seen. An example would be decreasing the amount of dense, tall vegetation in the landscaping so that attackers cannot conceal themselves within it, or placing critical resources in areas where intruders would have to cross over a wide, open space to reach them (making it likely that someone would notice them).

Security lighting

Security lighting is another effective form of deterrence. Intruders are less likely to enter well-lit areas for fear of being seen. Doors, gates, and other entrances, in particular, should be well lit to allow close observation of people entering and exiting. When lighting the grounds of a facility, widely-distributed low-intensity lighting is generally superior to small patches of high-intensity lighting, because the latter can have a tendency to create blind spots for security personnel and CCTV cameras. It is important to place lighting in a manner that makes it difficult to tamper with (e.g. suspending lights from tall poles), and to ensure that there is a backup power supply so that security lights will not go out if the electricity is cut off.*[10]

2.2.2 Intrusion detection and electronic surveillance

Main article: Surveillance

Alarm systems and sensors

Main article: CCTV
Main article: Security alarms

Alarm systems can be installed to alert security personnel when unauthorized access is attempted. Alarm systems work in tandem with physical barriers, mechanical systems, and security guards, serving to trigger a response when these other forms of security have been breached. They consist of sensors including motion sensors, contact sensors, and glass break detectors.*[11]

However, alarms are only useful if there is a prompt response when they are triggered. In the reconnaissance phase prior to an actual attack, some intruders will test the response time of security personnel to a deliberately tripped alarm system. By measuring the length of time it takes for a security team to arrive (if they arrive at all), the attacker

Fingerprint Residential Lock 2014

Closed-circuit television cameras

can determine if an attack could succeed before authorities arrive to neutralize the threat. Loud audible alarms can also act as a psychological deterrent, by notifying intruders that their presence has been detected.*[12] In some jurisdictions, law enforcement will not respond to alarms from intrusion detection systems unless the activation has been verified by an eyewitness or video.*[13] Policies like this one have been created to combat the 94–99 percent rate of false alarm activation in the United States.*[14]

Video surveillance

Main article: CCTV

Surveillance cameras can be a deterrent*[15] when placed in highly visible locations, and are also useful for incident verification and historical analysis. For example, if alarms are being generated and there is a camera in place, the camera could be viewed to verify the alarms. In instances when an attack has already occurred and a camera is in place at the point of attack, the recorded video can be reviewed. Although the term closed-circuit television (CCTV) is common, it is quickly becoming outdated as more video systems lose the closed circuit for signal transmission and are instead transmitting on IP camera networks.

Video monitoring does not necessarily guarantee that a human response is made to an intrusion. A human must be monitoring the situation realtime in order to respond in a timely manner. Otherwise, video monitoring is simply a means to gather evidence to be analyzed at a later time. However, advances in information technology are reducing the amount of work required for video monitoring, through automated video analytics.*[16]*[17]*[18]

2.2.3 Access control

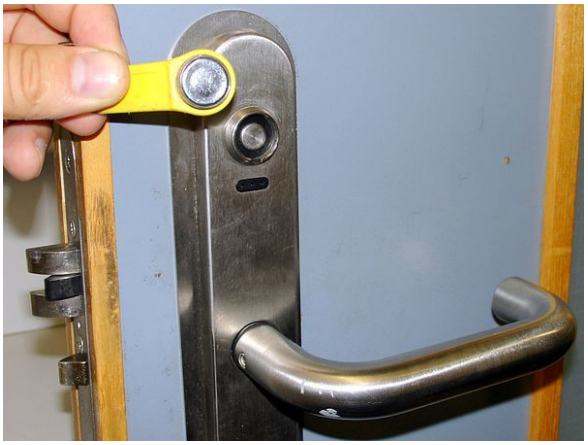
Main article: Access control

Access control methods are used to monitor and control traffic through specific access points and areas of the secure facility. This is done using a variety of systems including CCTV surveillance, identification cards, security guards, and electronic/mechanical control systems such as locks, doors, and gates.*[19]*[20]*[21]

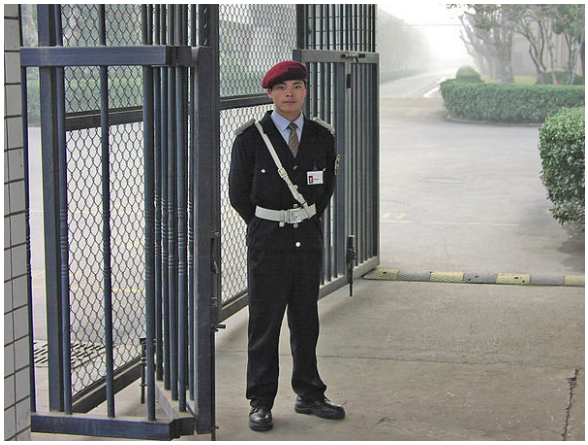
Mechanical access control systems

Main article: Lock (security device)

Mechanical access control systems include gates, doors, and locks. Key control of the locks becomes a problem with large user populations and any user turnover. Keys quickly become unmanageable, often forcing the adoption of electronic access control.



An electronic access control system, controlling entry through a door.



Private factory guard

Electronic access control systems

Electronic access control manages large user populations, controlling for user lifecycles times, dates, and individual access points. For example a user's access rights could allow access from 0700h to 1900h Monday through Friday and expires in 90 days.

An additional sub-layer of mechanical/electronic access control protection is reached by integrating a key management system to manage the possession and usage of mechanical keys to locks or property within a building or campus.

Identification systems and access policies

Another form of access control (*procedural*) includes the use of policies, processes and procedures to manage the ingress into the restricted area. An example of this is the deployment of security personnel conducting checks for authorized entry at predetermined points of entry. This form of access control is usually supplemented by the earlier forms of access control (i.e. mechanical and electronic access control), or simple devices such as physical passes.

2.2.4 Security personnel

Main article: Security guard

Security personnel play a central role in all layers of security. All of the technological systems that are employed to enhance physical security are useless without a security force that is trained in their use and maintenance, and which knows how to properly respond to breaches in security. Security personnel perform many functions: as patrols and at checkpoints, to administer electronic access control, to respond to alarms, and to monitor and analyze video.*[22]

2.3 See also

- Alarm management
- Biometrics
- Boundaries of Security Report
- Burglar alarm
- Computer security
- Door security
- Executive protection
- Guard tour patrol system
- Information security
- Logical security
- Physical Security Professional
- School security
- Security engineering
- Surveillance

2.4 References

[1] "Chapter 1: Physical Security Challenges". *Field Manual 3-19.30: Physical Security*. Headquarters, United States Department of Army. 2001.

[2] Garcia, Mary Lynn (2007). *Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann. pp. 1–11. ISBN 9780080554280.

[3] "Chapter 2: The Systems Approach". *Field Manual 3-19.30: Physical Security*. Headquarters, United States Department of Army. 2001.

[4] Anderson, Ross (2001). *Security Engineering*. Wiley. ISBN 978-0-471-38922-4.

[5] For a detailed discussion on natural surveillance and CPTED, see Fennelly, Lawrence J. (2012). *Effective Physical Security*. Butterworth-Heinemann. pp. 4–6. ISBN 9780124158924.

[6] Task Committee; Structural Engineering Institute (1999). *Structural Design for Physical Security*. ASCE. ISBN 978-0-7844-0457-7.

[7] Baker, Paul R. (2012). "Security Construction Projects". In Baker, Paul R. & Benny, Daniel J. *The Complete Guide to Physical Security*. CRC Press. ISBN 9781420099638.

[8] "Chapter 4: Protective Barriers". *Field Manual 3-19.30: Physical Security*. Headquarters, United States Department of Army. 2001.

[9] Talbot, Julian & Jakeman, Miles (2011). *Security Risk Management Body of Knowledge*. John Wiley & Sons. pp. 72–73. ISBN 9781118211267.

[10] Kovacich, Gerald L. & Halibozek, Edward P. (2003). *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*. Butterworth-Heinemann. pp. 192–193. ISBN 9780750674874.

[11] "Chapter 6: Electronic Security Systems". *Field Manual 3-19.30: Physical Security*. Headquarters, United States Department of Army. 2001.

[12] Fennelly, Lawrence J. (2012). *Effective Physical Security*. Butterworth-Heinemann. pp. 345–346. ISBN 9780124158924.

[13] "Evaluation of alternative policies to combat false emergency calls". p. 238.

[14] "Evaluation of alternative policies to combat false emergency calls". p. 233.

[15] "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention".

[16] Crowell, William P. et al (2011). "Intelligent Video Analytics". In Cole, Eric. *Physical and Logical Security Convergence*. Syngress. ISBN 9780080558783.

[17] Dufour, Jean-Yves (2012). *Intelligent Video Surveillance Systems*. John Wiley & Sons. ISBN 9781118577868.

[18] Caputo, Anthony C. (2010). *Digital Video Surveillance and Security*. Butterworth-Heinemann. ISBN 9780080961699.

[19] Tyska, Louis A. & Fennelly, Lawrence J. (2000). *Physical Security: 150 Things You Should Know*. Butterworth-Heinemann. p. 3. ISBN 9780750672559.

[20] "Chapter 7: Access Control". *Field Manual 3-19.30: Physical Security*. Headquarters, United States Department of Army. 2001.

[21] Pearson, Robert (2011). "Chapter 1: Electronic Access Control". *Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions*. Butterworth-Heinemann. ISBN 9780080494708.

[22] Reid, Robert N. (2005). "Guards and guard forces". *Facility Manager's Guide to Security: Protecting Your Assets*. The Fairmont Press. ISBN 9780881734836.

Chapter 3

Closed-circuit television

"CCTV" redirects here. For the Chinese television network, see China Central Television. For closed-circuit screenings for an audience, see Public and private screening. For other uses, see CCTV (disambiguation).

Closed-circuit television (**CCTV**), also known as **video surveillance**, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores. Videotelephony is seldom called "CCTV" but the use of video in distance education, where it is an important tool, is often so called.*[1]*[2]

Surveillance cameras on the corner of a building.

Dome CCTV cameras.

In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing digital video recorders*[3] (DVRs), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as motion detection and email alerts). More recently, decentralized IP cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for completely stand-alone operation. Surveillance of the public using CCTV is particularly common in many areas around the world. In recent years, the use of body worn video cameras has been introduced as a new form of surveillance.

3.1 History

The first CCTV system was installed by Siemens AG at Test Stand VII in Peenemünde, Germany in 1942, for observing the launch of V-2 rockets.*[4] The noted German engineer Walter Bruch was responsible for the technological design and installation of the system.*[note 1]

In the U.S. the first commercial closed-circuit television system became available in 1949, called Vericon. Very little is known about Vericon except it was advertised as not requiring a government permit.*[8]

Closed circuit TV in Munich, 1973 photo

Sign warning that premises are watched by CCTV cameras.

3.1.1 Technology

The earliest video surveillance systems involved constant monitoring because there was no way to record and store information. The development of reel-to-reel media enabled the recording of surveillance footage. These systems required magnetic tapes to be changed manually, which was a time consuming, expensive and unreliable process, with the operator having to manually thread the tape from the tape reel through the recorder onto an empty take-up reel. Due to these shortcomings, video surveillance was not widespread. VCR technology became available in the 1970s, making it easier to record and erase information, and use of video surveillance became more common.*[9]

During the 1990s, digital multiplexing was developed, alloweding several cameras to record at once, as well as time lapse and motion-only recording. This increased savings of time and money and the led to an increase in the use of CCTV.*[10]

Recently CCTV technology has been enhanced with a shift towards internet-based products and systems, and other technological developments.

3.1.2 Application

In September 1968, Olean, New York was the first city in the United States to install video cameras along its main business street in an effort to fight crime.*[11] Another early appearance was in 1973 in Times Square in New York City.*[12] The NYPD installed it in order to deter crime that was occurring in the area; however, crime rates did not appear to drop much due to the cameras.*[12] Nevertheless, during the 1980s video surveillance began to spread across the country specifically targeting public areas.*[10] It was seen as a cheaper way to deter crime compared to increasing the size of the police departments.*[12] Some businesses as well, especially those that were prone to theft, began to use video surveillance.*[12] From the mid-1990s on, police departments across the country installed an increasing number of cameras in various public spaces including housing projects, schools and public parks departments.*[12] CCTV later became common in banks and stores to discourage theft, by recording evidence of criminal activity. In 1998, 3,000 CCTV systems were in use in New York City.*[13]

Experiments in the UK during the 1970s and 1980s, including outdoor CCTV in Bournemouth in 1985, led to several larger trial programs later that decade. The first use by local government was in King's Lynn, Norfolk, in 1987.*[14] These were deemed successful in the government report "CCTV: Looking Out For You", issued by the Home Office in 1994, and paved the way for an increase in the number of CCTV systems installed. Today, systems cover most town and city centres, and many stations, car-parks and estates.

3.2 Uses

3.2.1 Crime prevention

A 2009 analysis by Northeastern University and the University of Cambridge, "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis," examined 44 different studies that collectively surveyed areas from the United Kingdom to U.S. cities such as Cincinnati and New York.
The analysis found that:

The two year-old James Bulger being led away by his killers, recorded on shopping centre CCTV in 1993. This narrow-bandwidth television system had a low frame rate.

1. Surveillance systems were most effective in parking lots, where their use resulted in a 51% decrease in crime;

2. Public transportation areas saw a 23% decrease in crimes;

3. Systems in public settings were the least effective, with just a 7% decrease in crimes overall. When sorted by country, however, systems in the United Kingdom accounted for the majority of the decrease; the drop in other areas was insignificant.[*][15]

The results from the above 2009 "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis" ,[*][15][*][16] are somewhat controversial.[*][17] Earlier similar meta-analysis completed by Walsh and Farrington in 2002 showed similar results: a significant decrease in car park crime (41%), and a non-significant decrease of crime in public transit and public places.[*][18] This study was criticised for the inclusion of confounding variables (e.g. notification of CCTV cameras on site, improved street lighting) found in the studies analyzed (including car park studies). These factors could not be differentiated from the effect of CCTV cameras being present or absent while crimes were being committed.[*][16][*][17] Thus, a combination of factors might be important for the decrease in crime not just the CCTV cameras. The 2009 study admitted to similar problems as well as issues with the consistency of the percentage of area covered by CCTV cameras within the tested sites (e.g. car parks have more cameras per square inch than public transit).[*][16] There is still much research to be done to determine the effectiveness of CCTV cameras on crime prevention before any conclusions can be drawn.

Closed-circuit video cameras in the Navy Yard complex caught gunman Aaron Alexis during his shooting rampage.

There is strong anecdotal evidence that CCTV aids in detection and conviction of offenders; indeed UK police forces routinely seek CCTV recordings after crimes.[*][19] Moreover CCTV has played a crucial role in tracing the movements of suspects or victims and is widely regarded by antiterrorist officers as a fundamental tool in tracking terrorist suspects. Large-scale CCTV installations have played a key part of the defences against terrorism since the 1970s. Cameras have also been installed on public transport in the hope of deterring crime,[*][20][*][21] and in mobile police surveillance vehicles, often with automatic number plate recognition, and a network of APNI-linked cameras is used to manage London's congestion charging zone. Even so there is political hostility to surveillance and several commentators downplay the evidence of CCTV's effectiveness, especially in the US.[*][22] However, most of these assertions are based on poor methodology or imperfect comparisons.[*][23]

A more open question is whether most CCTV is cost-effective. While low-quality domestic kits are cheap the professional installation and maintenance of high definition CCTV is expensive.[*][24] Gill and Spriggs did a Cost-effectiveness analysis (CEA) of CCTV in crime prevention that showed little monetary saving with the installation of CCTV as most of the crimes prevented resulted in little monetary loss.[*][17] Critics however noted that benefits of non-monetary value cannot be captured in a traditional Cost Effectiveness Analysis and were omitted from their study.[*][17] A 2008 Report by UK Police Chiefs con-

cluded that only 3% of crimes were solved by CCTV.*[25] In London, a Metropolitan Police report showed that in 2008 only one crime was solved per 1000 cameras.*[26] In some cases CCTV cameras have become a target of attacks themselves.*[27]

Cities such as Manchester in the UK are using DVR-based technology to improve accessibility for crime prevention.*[28]

In October 2009, an "Internet Eyes" website was announced which would pay members of the public to view CCTV camera images from their homes and report any crimes they witnessed. The site aimed to add "more eyes" to cameras which might be insufficiently monitored. Civil liberties campaigners criticized the idea as "a distasteful and a worrying development".*[29]

In 2013 Oaxaca hired deaf police officers to lip read conversations to uncover criminal conspiracies.*[30]

3.2.2 Industrial processes

Industrial processes that take place under conditions dangerous for humans are today often supervised by CCTV. These are mainly processes in the chemical industry, the interior of reactors or facilities for manufacture of nuclear fuel. Special cameras for some of these purposes include line-scan cameras and thermographic cameras which allow operators to measure the temperature of the processes. The usage of CCTV in such processes is sometimes required by law.

3.2.3 Traffic monitoring

Main article: Traffic camera

Many cities and motorway networks have extensive traffic-monitoring systems, using closed-circuit television to detect congestion and notice accidents.*[31] Many of these cameras however, are owned by private companies and transmit data to drivers' GPS systems.

The UK Highways Agency has a publicly owned CCTV network of over 1,200 cameras covering the British motorway and trunk road network. These cameras are primarily used to monitor traffic conditions and are not used as speed cameras. With the addition of fixed cameras for the Active Traffic Management system, the number of cameras on the Highways Agency's CCTV network is likely to increase significantly over the next few years.

The London congestion charge is enforced by cameras positioned at the boundaries of and inside the congestion charge zone, which automatically read the licence plates of cars. If the driver does not pay the charge then a fine will be imposed. Similar systems are being developed as a means of locating cars reported stolen.

Other surveillance cameras serve as traffic enforcement cameras.

3.2.4 Transport safety

Digital Video Recorder for Public Transport

A CCTV system may be installed where an operator of a machine cannot directly observe people who may be injured by some unexpected machine operation. For example, on a subway train, CCTV cameras may allow the operator to confirm that people are clear of doors before closing them and starting the train.

Operators of an amusement park ride may use a CCTV system to observe that people are not endangered by starting the ride. A CCTV camera and dashboard monitor can make reversing a vehicle safer, if it allows the driver to observe objects or people not otherwise visible.

3.2.5 Control of retail

Someas software integrate with CCTV to monitor the actions of workers in retail environments. Every action is recorded as an information block with subtitles that explain the performed operation. This helps to track the actions of workers, especially when they are making critical financial transactions, such as correcting or cancelling of a sale, withdrawing money or altering personal information.

Actions which an employer may wish to monitor could include:

- Scanning of goods, selection of goods, introduction of price and quantity;
- Input and output of operators in the system when entering passwords;
- Deleting operations and modifying existing documents;

- Implementation of certain operations, such as financial statements or operations with cash;
- Moving goods, revaluation scrapping and counting;
- Control in the kitchen of fast food restaurants;
- Change of settings, reports and other official functions.

Each of these operations is transmitted with a description, allowing detailed monitoring of all actions of the operator. Some systems allow the user to search for a specific event by time of occurrence and text description, and perform statistical evaluation of operator behaviour. This allows the software to predict deviations from the standard workflow and record only anomalous behaviour.

3.2.6 Use in schools

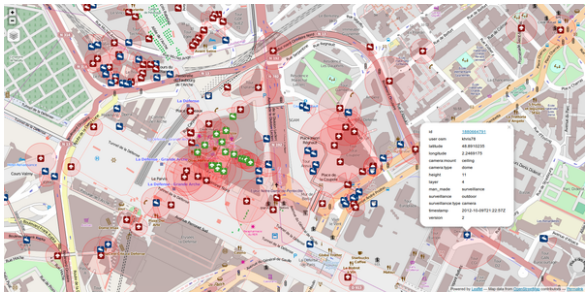
Eric Harris and Dylan Klebold caught on the cafeteria's security cameras during the Columbine High School Massacre

In the United States and other places, CCTV may be installed in school to monitor visitors, track unacceptable student behavior and maintain a record of evidence in the event of a crime. There are some restrictions on installation, with cameras not being installed in an area where there is a "reasonable expectation of privacy", such as bathrooms, gym locker areas and private offices (unless consent by the office occupant is given). Cameras are generally acceptable in hallways, parking lots, front offices where students, employees, and parents come and go, gymnasiums, cafeterias, supply rooms and classrooms. The installation of cameras in classrooms may be objected to by some teachers.*[32]

3.2.7 Criminal use

Criminals may use surveillance cameras to monitor the public. For example, a hidden camera at an ATM can capture people's PINs as they are entered, without their knowledge. The devices are small enough not to be noticed, and are placed where they can monitor the keypad of the machine as people enter their PINs. Images may be transmitted wirelessly to the criminal.*[33]

3.3 Prevalence



A crowdsourced map of CCTV cameras near Grande Arche using OpenStreetMap data.[34]*

Surveillance camera mounted on the walls of Rosenbad, one of the Swedish's government buildings in central Stockholm, which houses the Prime Minister's office. One of the parliament's (Riksdagen) building can be seen in the background.

With lower cost and easier installation, sales of home security cameras in the United States increased in the early 21st century.*[35] Following the September 11 attacks, the use of video surveillance in public places became more common to deter future terrorist attacks.*[12] In 2010, there were more than 10,000 CCTV systems in Chicago, many linked to an integrated camera network.*[36]

In Latin America, the CCTV market is growing rapidly with the increase of property crime.*[37]

An article published in *CCTV Image* magazine estimated the number of cameras in the United Kingdom was 1.85 million in 2011. The estimate was based on extrapolating from a comprehensive survey of public and private cameras within the Cheshire Constabulary jurisdiction.*[38] This

A surveillance camera, aimed at a public street (Kungsgatan) in Stockholm, Sweden, mounted on top of the pole.

works out as an average of one camera for every 32 people in the UK, although the density of cameras varies greatly from place to place. The Cheshire report also claims that the average person on a typical day would be seen by 70 CCTV cameras.

The Cheshire figure is regarded as more dependable than a previous study by Michael McCahill and Clive Norris of UrbanEye published in 2002.*[39] Based on a small sample in Putney High Street, McCahill and Norris estimated the number of surveillance cameras in private premises in London at around 500,000 and the total number of cameras in the UK at around 4,200,000. According to their estimate the UK has one camera for every 14 people. Although it has been acknowledged for several years that the methodology behind this figure is flawed,*[40] it has been widely quoted.

The *CCTV User Group* estimated that were are around 1.5 million CCTV cameras in city centres, stations, airports, and major retail areas in the UK.*[41] This figure does not include the smaller surveillance systems such as those that may be found in local corner shops and is therefore broadly in line with the Cheshire report.

Research conducted by the Scottish Centre for Crime and Justice Research and based on a survey of all Scottish local authorities, identified that there are over 2,200 public space CCTV cameras in Scotland.*[42]

3.4 Privacy

A mobile closed-circuit TV van monitoring a street market

Opponents of CCTV point out the loss of privacy of people under surveillance, and the negative impact of surveillance on civil liberties. Furthermore, they argue that CCTV displaces crime, rather than reducing it. Critics often dub CCTV as "Big Brother surveillance", a reference to George Orwell's novel *Nineteen Eighty-Four*, which featured a two-way telescreen in every home through which The Party would monitor the populace. Civil liberties campaign group Big Brother Watch have published several research papers into CCTV systems. In December 2009, they released a report documenting council controlled CCTV cameras.*[43]

In the United State of America, video surveillance may require a judges writ, which is readily available.*[44]

Proponents of CCTV cameras have argued that the cameras are not intruding into people's privacy, as they are not surveilling private, but *public* space, where an individual's right to privacy can reasonably be weighed against the benefits of surveillance.*[45] However, anti-surveillance activists have held that there is a right to privacy in public areas. Furthermore, while it is true that there may be scenarios wherein a person's right to public privacy can be both reasonably and justifiably compromised, some scholars have argued that such situations are so rare as to not sufficiently warrant the frequent compromising of public pri-

vacy rights that occurs in regions with widespread CCTV surveillance. For example, in her book *Setting the Watch: Privacy and the Ethics of CCTV Surveillance*, Beatrice von Silva-Tarouca Larsen argues that CCTV surveillance is ethically permissible only in "certain restrictively defined situations", such as when a specific location has a "comprehensively documented and significant criminal threat". [46] Her central reasoning is that widespread CCTV surveillance violates citizens' rights to privacy and anonymity within the public sphere by jeopardizing both their liberty and dignity. She concludes that CCTV surveillance should therefore be reserved for specific circumstances in which there are clear and reasonably demonstrated benefits to its implementation and few ethical compromises.

Questions are also raised about illegal access to CCTV recordings. The Data Protection Act 1998 in the United Kingdom led to legal restrictions on the uses of CCTV recordings, and also mandated their registration with the Data Protection Agency. In 2004, the successor to the Data Protection Agency, the Information Commissioner's Office clarified that this required registration of all CCTV systems with the Commissioner, and prompt deletion of archived recordings. However, subsequent case law (Durant vs. FSA) limited the scope of the protection provided by this law, and not all CCTV systems are currently regulated. [47] However, private sector personnel in the UK who operate or monitor CCTV devices or systems are considered security guards and have been made subject to state licensing.

A 2007 report by the UK Information Commissioner's Office, highlighted the need for the public to be made more aware of the "creeping encroachment" into their civil liberties created by the growing use of surveillance. [48] [49] In the same year, the UK watchdog CameraWatch claimed that the majority of CCTV cameras in the UK are operated illegally or are in breach of privacy guidelines. [50] In response, the Information Commissioner's Office denied the claim adding that any reported abuses of the Data Protection Act are swiftly investigated. [50]

The UK Home Office published a code of practice in 2013 for the use of surveillance cameras by government and local authorities. The aim of the code is to help ensure their use is "characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator. Surveillance by consent should be regarded as analogous to policing by consent." [51]

In Canada, the use of video surveillance has grown very rapidly. In Ontario, both the *municipal* and *provincial* versions of the Freedom of Information and Protection of Privacy Act outline very specific guidelines that control how *images* and *information* can be gathered by this method and or released. [52]

3.5 Technological developments

Surveillance camera at London Heathrow Airport with a wiper for clear images during rain

3.5.1 Computer controlled analytics and identification

Computer controlled cameras can identify, track, and categorize objects in their field of view.

Video Content Analysis (VCA) is the capability of automatically analyzing video to detect and determine temporal events not based on a single image. As such, it can be seen as the automated equivalent of the biological visual cortex.

A system using VCA can recognize changes in the environment and even identify and compare objects in the database using size, speed, and sometimes colour. The camera's actions can be programmed based on what it is "seeing". For example; an alarm can be issued if an object has moved in a certain area, or if a painting is missing from a wall, or if a smoke or fire is detected, or if running people are detected, or if fallen people are detected and if someone has spray painted the lens, as well as video loss, lens cover, defocuss and other so called camera tampering events.

VCA analytics can also be used to detect unusual patterns in an environment. The system can be set to detect anomalies in a crowd, for instance a person moving in the opposite direction in airports where passengers are only supposed to walk in one direction out of a plane or in a subway where people are not supposed to exit through the entrances. [53]

VCA can track people on a map by calculating their position from the images. It is then possible to link many cameras and track a person through an entire building or area. This

can allow a person to be followed without having to analyze many hours of film. Currently the cameras have difficulty identifying individuals from video alone, but if connected to a key-card system, identities can be established and displayed as a tag over their heads on the video.

There is also a significant difference in where the VCA technology is placed, either the data is being processed within the cameras (on the edge) or by a centralized server. Both technologies have their pros and cons.*[54]

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

The combination of CCTV and facial recognition has been tried as a form of mass surveillance, but has been ineffective because of the low discriminating power of facial recognition technology and the very high number of false positives generated. This type of system has been proposed to compare faces at airports and seaports with those of suspected terrorists or other undesirable entrants.

Eye-in-the-sky surveillance dome camera watching from a high steel pole

Computerized monitoring of CCTV images is under development, so that a human CCTV operator does not have to endlessly look at all the screens, allowing an operator to observe many more CCTV cameras. These systems do not observe people directly. Instead, they track their behavior by looking for particular types of body-movement behavior, or particular types of clothing or baggage.

To many, the development of CCTV in public areas, linked to computer databases of people's pictures and identity, presents a serious breach of civil liberties. Conservative critics fear the possibility that one would no longer have anonymity in public places.*[55] Demonstrations or assemblies in public places could be affected as the state would be able to collate lists of those leading them, taking part, or even just talking with protesters in the street.

Comparatively harmless are people counter systems. They use CCTV equipment as front end eyes of devices which perform shape recognition technology in order to identify objects as human beings and count people passing predefined areas.

3.5.2 Retention, storage and preservation

Most CCTV systems may record and store digital video and images to a digital video recorder (DVR) or, in the case of IP cameras, directly to a server, either on-site or offsite.

There is a cost in the retention of the images produced by CCTV systems. The amount and quality of data stored on storage media is subject to compression ratios, images stored per second, image size and is effected by the retention period of the videos or images.*[56] DVRs store images in a variety of proprietary file formats. Recordings may be retained for a preset amount of time and then automatically archived, overwritten or deleted, the period being determined by the organisation that generated them.

3.5.3 Closed-circuit digital photography (CCDP)

See also: Closed-circuit television camera

Closed-circuit digital photography (CCDP) is more suited for capturing and saving recorded high-resolution photographs, whereas closed-circuit television (CCTV) is more suitable for live-monitoring purposes.

However, an important feature of some CCTV systems is the ability to take high resolution images of the camera scene, e.g. on a time lapse or motion-detection basis. Images taken with a digital still camera often have higher resolution than those taken with some video cameras. Increas-

ingly, low-cost high-resolution digital still cameras can also be used for CCTV purposes.

Images may be monitored remotely when the computer is connected to a network.

3.5.4 IP cameras

Main article: IP camera

A growing branch in CCTV is *internet protocol* cameras (IP cameras). IP cameras use the Internet Protocol (IP) used by most Local Area Networks (LANs) to transmit video across data networks in digital form. IP can optionally be transmitted across the public internet, allowing users to view their cameras through any internet connection available through a computer or a 3G phone. For professional or public infrastructure security applications, IP video is restricted to within a private network or VPN,* [57] or can be recorded onto a remote server.

Easy Connect Wireless IP camera

3.5.5 Networking CCTV cameras

The city of Chicago operates a networked video surveillance system which combines CCTV video feeds of government agencies with those of the private sector, installed in city buses, businesses, public schools, subway stations, housing projects etc. Even home owners are able to contribute footage. It is estimated to incorporate the video feeds of a total of 15,000 cameras.

The system is used by Chicago's Office of Emergency Management in case of an emergency call: it detects the caller's location and instantly displays the real-time video feed of the nearest security camera to the operator, not requiring any user intervention. While the system is far too vast to allow complete real-time monitoring, it stores the video data for later usage in order to provide possible evidence in criminal cases.* [58]

London also has a network of CCTV systems that allows multiple authorities to view and control CCTV cameras in real time. The system allows authorities including the Metropolitan Police Service, Transport for London and a number of London boroughs to share CCTV images between them. It uses a network protocol called Television Network Protocol to allow access to many more cameras than each individual system owner could afford to run and maintain.

The Glynn County Police Department uses a wireless mesh-networked system of portable battery-powered tripods for live megapixel video surveillance and central monitoring of tactical police situations. The systems can be used either on a stand-alone basis with secure communications to nearby police laptops, or within a larger mesh system with multiple tripods feeding video back to the command vehicle via wireless, and to police headquarters via 3G.

3.5.6 Integrated systems

Integrated systems allow users to connect remotely from the internet and view what their cameras are viewing remotely, similar to that of IP cameras. In one incident in 2009, a lady from Boynton Beach, Florida was able to watch her house get burgled and contacted police directly from her office at work.* [59]

3.5.7 Wireless security cameras

Main article: Wireless security camera

Many consumers are turning to wireless security cameras for home surveillance. Wireless cameras do not require a video cable for video/audio transmission, simply a cable for power. Wireless cameras are also easy and inexpensive

An integrated systems unit.

Wireless security camera

to install. Previous generations of wireless security cameras relied on analog technology; modern wireless cameras use digital technology which delivers crisper audio, sharper video, and a secure and interference-free signal.*[60]

3.6 CCTV camera vandalism

Unless physically protected, CCTV cameras have been found to be vulnerable against a variety of (mostly illegal) tactics:

- Some people will deliberately destroy cameras. Some cameras can come with dust-tight, pressurized, explosion proof, and bullet-resistant housings.
- Spraying substances over the lens can make the image too blurry to view.
- Lasers can blind or damage them. However, since most lasers are monochromatic, color filters can reduce the effect of laser pointers. However, filters will also impair image quality and overall light sensitivity of cameras (see laser safety article for details on issues with filters). Also, complete protection from infrared, red, green, blue and UV lasers would require use of completely black filters, rendering the camera useless.

3.7 See also

- Bugging
- Closed-circuit television camera
- Documentary practice
- Eye in the sky (camera)
- Fake security camera
- Information Awareness Office
- IP camera
- Physical security
- Privacy International
- Proprietary DVR
- Physical Security Information Management - PSIM
- Security Operations Center
- Security smoke
- Sousveillance (inverse surveillance)
- Surveillance
- Telescreen
- The Convention on Modern Liberty
- TV Network Protocol
- Under vehicle inspection
- Video analytics
- Videotelephony
- Washington County Closed-Circuit Educational Television Project

3.8 Notes

[1] CCTV recording systems are still often used at modern launch sites to record the flight of the rockets, in order to find the possible causes of malfunctions,*[5]*[6] while larger rockets often send pictures of stage separation back to earth by radio link.*[7]

3.9 References

[1] Verman, Romesh. Distance Education In Technological Age, Anmol Publications Pvt. Ltd., 2005, pp.166, ISBN 81-261-2210-2, ISBN 978-81-261-2210-3.

[2] "Distance education in Asia and the Pacific: Proceedings Of The Regional Seminar On Distance Education, 26 November - 3 December 1986", Asian Development Bank, Bangkok, Thailand, Volume 2, 1987

[3] "CCTV Digital Video Recorders (DVRs)". sourcesecurity.com. Retrieved 29 June 2013.

[4] Dornberger, Walter: *V-2*, Ballantine Books 1954, ASIN: B000P6L1ES, page 14.

[5] "ET_SRB Cam FS.indd" (PDF). Retrieved 2009-07-22.

[6] "Ecliptic Enterprises Corporation". Eclipticenterprises.com. Archived from the original on July 5, 2008. Retrieved 2009-05-08.

[7] Brent D. Johnson. "Cameras Monitor Rocket Launch". Photonics.com. Retrieved 2009-05-08.

[8] "*Television Rides Wires*", February 1949, Popular Science small article, bottom of page 179

[9] CCTV Surveillance: Video Practices and Technology

[10] [Roberts, Lucy. "History of Video Surveillance and CCTV" We C U Surveillance http://www.wecusurveillance.com/cctvhistory Retrieved 2011-10-20]

[11] [Robb, Gary C. (1979) "Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations" University of Michigan Journal of Law Reform. pg. 572]

[12] [Yesil, Bilge. (2006) "Watching Ourselves" Cultural Studies. Vol 20(4-5) pg. 400-416]

[13] "You're being watched, New York!". BBC. 11 March 2002.

[14] Staff (August 2007). "CCTV". Borough Council of King's Lynn & West Norfolk. Retrieved 2008-12-14.

[15] "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis". Journalist's Resource.org.

[16] Walsh B.C.,Farrington D.P. (2009). "Public area CCTV and crime prevention: An updated systematic review and meta-analysis". *Justice Quarterly* **26** (4): 716–745. doi:10.1080/07418820802506206.

[17] "Assessing the impact of CCTV" (PDF). Retrieved 2011-10-16.

[18] Walsh B.C.,Farrington D.P. (2009). "Effects of closed-circuit television on crime". *The Annals of the American Academy of Political and Social Science* **587** (1): 110–135. doi:10.1177/0002716202250802.

[19] "Police are failing to recover crucial CCTV footage, new figures suggest.," *The Telegraph*

[20] "CCTV to drive down cab attacks," *BBC*

[21] Taxi CCTV cameras are installed," *BBC*

[22] Baram, Marcus (2007-07-09). "Eye on the City: Do Cameras Reduce Crime?". *ABC News*. Retrieved 2007-07-10.

[23] "Tens of thousands of CCTV cameras, yet 80% of crime unsolved" by Justin Davenport 2007

[24] "National community Crime Prevention Programme" (PDF). Retrieved 2011-10-16.

[25] "Are CCTV cameras a waste of money in the fight against crime?" Forward Edge, 7 May 2008

[26] Hughe, Mark (25 August 2009). "CCTV in the spotlight: one crime solved for every 1,000 cameras". Independent News and Media Limited. Retrieved 2009-08-27.

[27] "http://news.bbc.co.uk/," *BBC*

[28] "Digital CCTV Scheme Switches On," *BBC*

[29] Public to Monitor CCTV From Home, *BBC*

[30] Angels of Silence see crime where others don't Globe & Mail, 20 Nov 2013

[31] Motorway Cameras in England, http://www.motorwaycameras.co.uk

[32] "Legal aspects of the use of video cameras in schools =".

[33] "ATM Security". Dedham Savings. Retrieved 2009-04-18.

[34] khris78. "The CCTV Map". *osmcamera*. Retrieved 2 August 2014.

[35] Home Security Camera Sales Rise cepro.com

[36] "Chicago Links Police, Private Cameras". WLS-TV. 2010. Retrieved 2010-08-16.

[37] "Latin American Physical Security Market Growing Rapidly," 8 October 2009 *Security Magazine*

[38] "Only 1.85 million cameras in UK, claims ACPO lead on CCTV - SecurityNewsDesk.com". SecurityNewsDesk.com. Retrieved 2011-03-02.

[39] "CCTV in London" (PDF). Retrieved 2009-07-22.

[40] "FactCheck: how many CCTV cameras? - Channel 4 News". Channel4.com. Retrieved 2009-05-08.

[41] "How many cameras are there?". CCTV User Group. 2008-06-18. Retrieved 2009-05-08.

[42] Bannister, J., Mackenzie, S. and Norris, P. Public Space CCTV in Scotland(2009), Scottish Centre for Crime and Justice Research (Research Report)

[43] "Councils 'treble CCTV in decade'". *BBC News*. 2009-12-18.

[44] Department of Justice - Video Surveillance Retrieved August 6, 1982

[45] *Smile, the cameras are here to watch over you - The New Zealand Herald*, Tuesday 18 March 2008, Page A14

[46] Von Silva-Tarouca Larsen, Beatrice (2011). *Setting the watch: Privacy and the ethics of CCTV surveillance*. Hart Publishing. p. 160. ISBN 978-1849460842.

[47] "Memorandum by A A Adams, BSc, MSc, PhD, LLM, MBCS, CITP School of Systems Engineering". *UK Parliament Constitution Committee - Written Evidence. Surveillance: Citizens and the State*. January 2007.

[48] "Privacy watchdog wants curbs on surveillance". The Telegraph. 1 May 2007.

[49] "CCTV, computers and the 'climate of fear'". Evening Standard. 30 April 2007.

[50] "Majority of UK's CCTV cameras 'are illegal'". The Telegraph. 31 May 2007.

[51] "Surveillance Camera Code of Practice". UK Government Home Office. June 2013. p. 5. Retrieved 1 December 2013.

[52] Freedom of Information and Protection of Privacy Act Text

[53] "MATE's Analytics Integrate with Hirsch Security Systems". Retrieved 2011-03-28.

[54] "Image Processing Techniques for Video Content Extraction" (PDF). Retrieved 2011-03-28.

[55] Todd Lewan (July 7, 2007). "Microchips in humans spark privacy debate". USAToday. Retrieved 2012-06-07.

[56] "MotionJPEG, JPEG2000, H.264 and MPEG-4 compression methods in CCTV". Retrieved 2011-05-01.

[57] "Some IP Cameras Can Be Remotely Monitored With An iPhone And Other Compatible 3G Devices" (PDF). Retrieved 2009-07-22.

[58] "Chicago's Camera Network Is Everywhere", *The Wall Street Journal*

[59] Kim Segal (April 10, 2009). "Woman watches home invasion on webcam". CNN. Retrieved 2009-05-08.

[60] *Digital Video Essentials: Shoot, Transfer, Edit, Share By Erica Sadun*. Retrieved 16 October 2013.

3.10 Further reading

- Armstrong, Gary, ed. (1999). *The maximum surveillance society: the rise of CCTV*. Berg (originally, University of Michigan Press). ISBN 9781859732212.
- Fyfe, Nicholas & Bannister, Jon (2005). "City Watching: Closed-Circuit Television in Public Spaces". In Fyfe, Nicholas & Kenny, Judith T. *The Urban Geography Reader*. Psychology Press. ISBN 9780415307017.
- Newburn, Tim & Hayman, Stephanie (2001). *Policing, Surveillance and Social Control: CCTV and police monitoring of suspects*. Taylor & Francis. ISBN 9781843924692.
- Norris, Clive (2003). "From Personal to Digital: CCTV, the panopticon, and the technological mediation of suspicion and social control". In Lyon, David. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Psychology Press. ISBN 9780415278737.

3.11 External links

- Space Shuttle External Tank and Solid Rocket Booster Camera Systems
- UK Government pro-CCTV campaign
- Assessing the Impact of CCTV, a UK Home office study on the effectiveness of closed-circuit television
- The Register story: Face recognition useless for crowd surveillance
- CCTV Guidance notes from the UK Information Commissioner's Office
- CBC Digital Archives - The Long Lens of the Law
- The Urbaneye Project on CCTV in Europe
- Monitoring of Security Camera
- CCTV:Constant Cameras Track Violators National Institute of Justice Journal 249 (2003). Washington, DC: U.S. Department of Justice.
- Public Space CCTV in Scotland: Results of a National Survey of Scotland's Local Authorities
- Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights and Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and the Protection of Human Rights, Venice Commission, 2007

Chapter 4

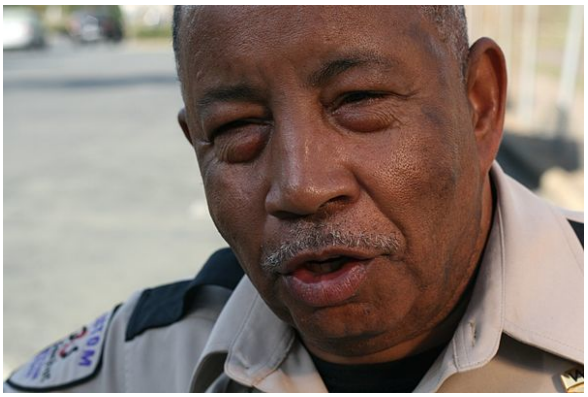
Security guard

"Mall cop" redirects here. For the movie, see Paul Blart: Mall Cop.

A **security officer** (or **security guard**) is a person who is paid to protect property, assets, or people. They are usually privately and formally employed civilian personnel. Security officers are generally uniformed and act to protect property by maintaining a high visibility presence to deter illegal and inappropriate actions, observing (either directly, through patrols, or by watching alarm systems or video cameras) for signs of crime, fire or disorder; then taking action and reporting any incidents to their client and emergency services as appropriate.

Until the 1980s, the term **watchman** was more commonly applied to this function, a usage dating back to at least the Middle Ages in Europe. This term was carried over to North America where it was interchangeable with **night-watchman** until both terms were replaced with the modern security-based titles. Security guards are sometimes regarded as fulfilling a private policing function.

4.1 Functions and duties



An American security guard at a North Carolina apartment complex in April 2010.

Many security firms and proprietary security departments practice the "detect, deter, observe and report" methodology. Security officers are not required to make arrests, but have the authority to make a citizen's arrest, or otherwise act as an agent of law enforcement, for example, at the request of a police officer or sheriff.

A private security officer's primary duty is the prevention and deterrence of crime. Security personnel enforce company rules and can act to protect lives and property, and they often have a contractual obligation to provide these actions. In addition to basic deterrence, security officers are often trained to perform specialized tasks such as arrest and control (including handcuffing and restraints), operate emergency equipment, perform first aid, CPR, take accurate notes, write detailed reports, and perform other tasks as required by the client they are serving.

All security officers are also required to go through additional training mandated by the state for the carrying of weapons such as batons, firearms, and pepper spray (e.g. the Bureau of Security and Investigative Services in California has requirements that a license for *each* item listed must be carried while on duty).[*][1] Some officers are required to complete police certification for special duties. Virginia training standards for security are identical to police training with regards to firearms (shotgun and handgun) but do not place licensing requirements for other items carried, only that training be provided that is documented. Several security companies have also become certified in RADAR and trained their sworn special police officers to use it on protected properties in conjunction with lights/sirens, allowing them to legally enforce traffic laws on private property.[*][2]

The number of jobs is expected to grow in the U.S., with 175,000 new security jobs expected before 2016.[*][3] In recent years, due to elevated threats of terrorism, most security officers are required to have bomb-threat training and/or emergency crisis training, especially those located in soft target areas such as shopping malls, schools, and any other area where the general public congregate.

One major economic justification for security personnel is that insurance companies (particularly fire insurance carriers) will give substantial rate discounts to sites which have a 24-hour presence. For a high risk or high value property, the discount can often exceed the money being spent on its security program. Discounts are offered because having security on site increases the odds that any fire will be noticed and reported to the local fire department before a total loss occurs. Also, the presence of security personnel (particularly in combination with effective security procedures) tends to diminish "shrinkage", theft, employee misconduct and safety rule violations, property damage, or even sabotage. Many casinos hire security guards to protect money when transferring it from the casino to the casino's bank.

Security personnel may also perform access control at building entrances and vehicle gates; meaning, they ensure that employees and visitors display proper passes or identification before entering the facility. Security officers are often called upon to respond to minor emergencies (lost persons, lockouts, dead vehicle batteries, etc.) and to assist in serious emergencies by guiding emergency responders to the scene of the incident, helping to redirect foot traffic to safe locations, and by documenting what happened on an incident report.

Armed security officers are frequently contracted to respond as law enforcement until a given situation at a client location is under control and/or public authorities arrive on the scene.

Patrolling is usually a large part of a security officer's duties. Often these patrols are logged by use of a guard tour patrol system, which require regular patrols. Until recently the most commonly used form used to be mechanical clock systems that required a key for manual punching of a number to a strip of paper inside with the time pre-printed on it. But recently, electronic systems have risen in popularity due to their light weight, ease of use, and downloadable logging capabilities.*[4] Regular patrols are, however, becoming less accepted as an industry standard, as it provides predictability for the would-be criminal, as well as monotony for the security officer on duty. Random patrols are easily programmed into electronic systems, allowing greater freedom of movement and unpredictability. Global positioning systems are beginning to be used because they are a more effective means of tracking officers' movements and behavior.

4.2 Personnel

Although security officers differ greatly from police officers, military personnel, federal agents/officers, and the like, Australia and the United States have a growing proportion of security personnel that have former police or military experience, including senior management personnel. On the other hand, some security officers, young people in particular, use the job as practical experience to use in applying to law enforcement agencies.

4.2.1 Types of security personnel and companies

A security guard protecting the entrance to an apartment building, and managing the parking of cars in Haikou, Hainan Province, China.

Security personnel are classified as either of the following:

- "In-house" or "proprietary" (i.e. employed by the same company or organization they protect, such as a mall, theme park, or casino); formerly often called works police or security police in the United Kingdom.
- "Security supervisor", meets with clients and employees as necessary to ensure client and employee satisfaction.*[5]
- "Scheduler" , Security Officer assignment and strategic scheduling resulting in client satisfaction, employee retention and cost maintained within District financial plans.*[6]

- "Human Resources Manager", effective delivery of human resources services such as employment, employee/labor relations, compensation, benefits administration, training and development, workers' compensation, and audit compliance. Maintains and implements corporate policies and programs related to employment.*[7]
- "Client Service Manager", promotes financial growth for the District by ensuring client retention, Security Officer retention, and support for the development of new business.*[8]
- "Client Service Supervisor", provides security services for designated clients resulting in customer satisfaction, Security Officer retention, and financial growth for the District. Provides service in a large and complex area.*[9]
- "Contract", working for a private security company which protects many locations.
- "Public Security", a person employed or appointed as an (usually armed) security officer by a government or government agency.
- "Private Police Officers", or "Special Police".
- "Private Patrol Officers", vehicle patrol officers that protect multiple client premises.
- "Parapolice", aggressive firms that routinely engage in criminal investigation and arrest.*[10]*[11]*[12]

Industry terms for security personnel include: security guard, security officer, security agent, safety patrol, private police, company police, security enforcement officer, and public safety. Terms for specialized jobs include bouncer, bodyguards, executive protection agent, loss prevention, alarm responder, hospital security officer, mall security officer, crime prevention officer, patrolman, private patrol officer, and private patrol operator.

State and local governments sometimes regulate the use of these terms by law—for example, certain words and phrases that "give an impression that he or she is connected in any way with the federal government, a state government, or any political subdivision of a state government" are forbidden for use by California security licensees by Business and Professions Code Section 7582.26. So the terms "private homicide police" or "special agent" would be unlawful for a security licensee to use in California. Similarly, in Canada, various acts*[13]*[14] specifically prohibits private security personnel from using the terms *Probation Officer*, *law enforcement*, *police*, or *police officer*.

Alberta and Ontario prohibit the use of the term *Security Officer*, which has been in widespread use in the United States for many decades. Recent changes to the act have also introduced restrictions on uniform and vehicle colours and markings to make private security personnel clearly distinctive from police personnel. Some sources feel that some of these restrictions are put in place to satisfy the Canadian Police Association.*[15]

Cash in transit van with a crew of security guards in Guangzhou, China

There is a marked difference between persons performing the duties historically associated with watchmen and persons who take a more active role in protecting persons and property. The former, often called "guards", are taught the mantra "observe and report", are minimally trained, and not expected to deal with the public or confront criminals.

The latter are often highly trained, sometimes armed depending on contracts agreed upon with clientele, and are more likely to interact with the general public and to confront the criminal element. These employees tend to take pride in the title "Security Officer" or "Protection Officer" and disdain the label of "guard".

Security jobs vary in pay and duties. There is sometimes little relationship between duties performed and compensation, for example some mall "security officers" who are exposed to serious risks earn less per hour than "industrial security guards" who have less training and responsibility.*[16] However, there are now more positions in the security role that separate not just the titles, but the job itself. The roles have progressed and so have the areas for which security people are needed.

The term "agent" can be confusing in the security industry because it can describe a civil legal relationship between an employee and their employer or contractor ("agent of the owner" in California PC 602), and also can describe a person in government service ("Special Agent Jones of the Federal Bureau of Investigation".) The title "agent" can be confused with bail enforcement agents, also known as

"bounty hunters", who are sometimes regulated by the same agencies which regulate private security. The term "agent" is also used in other industries, such as banking agents, loan agents and real estate agents.

Security agents are often employed in loss prevention and personal or executive protection (bodyguards) roles. They typically work in plainclothes (without a uniform), and are usually highly trained to act lawfully in direct defense of life or property.

Security personnel are essentially private citizens, and therefore are bound by the same laws and regulations as the citizenry they are contracted to serve, and therefore are not allowed to represent themselves as law enforcement under penalty of law.*[17]*[18]

4.3 Training

A Kenyan private security guard.

Just as with the police profession, training requirements for the private security industry have evolved over time.*[2] For many years security guards were poorly chosen and poorly trained (if at all), partly because security guard companies who contracted with clients in private industry were paid very little for their security guard services. For the most part, contracts were awarded to security guard companies through a competition process and the final selection was often made based on cost rather than the experience or professionalism of the security guard company. That changed drastically on September 11, 2001 when radical Islamic terrorists attacked the United States. The event moved corporate threat concerns to the top of the priority list for most security guard contracts started being awarded based on professionalism. More money was invested in security so more money became available for training of security guards. The term 'security professional' began to surface and large private security companies like Blackwater, USA began offering training services for the private security industry that approached the level of training provided by the military. Security guard companies began paying enough to attract people with significant backgrounds in law enforcement and the military, often in special operations.

4.3.1 Australia

Any person who conducts a business or is employed in a security-related field within Australia is required to be licensed. Each of the six states and two territories of Australia have separate legislation that covers all security activities. Licensing management in each state/territory is varied and is carried out by either Police, Attorney General's Department, Justice Department or the Department of Consumer Affairs.

- New South Wales —(Police) Security Industry Act 1997 & Security Industry Regulation 2007
- Victoria—(Police) Private Security Act 2004
- Queensland —(Justice & Attorney-General) Security Providers Act 1993
- South Australia—(Consumer & Business Affairs) Security and Investigation Agents Act 1995
- Western Australia—(Police) Security & Related Activities (Control) Act 1996 & Security & Related Activities (Control) Regulations 1997
- Tasmania —(Police) *Security and Investigation Agents Act 2002
- Northern Territory —(Justice) Private Security Act & Private Security (Security Officer/Crowd Controller/Security Firms/Miscellaneous Matters) Regulations;
- Australian Capital Territory —(Regulatory Services) Security Industry Act 2003 & Security Industry Regulation 2003

All of this legislation was intended to enhance the integrity of the private security industry.

All persons licensed to perform security activities are required to undertake a course of professional development in associated streams that are recognised nationally. This has not always been the case and the introduction of this requirement is expected to regulate the educational standards and knowledge base so that the particular job can be competently performed.

Strict requirements are laid down as to the type of uniform and badge used by security companies. Uniforms or badges that may be confused with a police officer are prohibited. Also, the use of the titles 'Security Police' or 'Private Detective' are unacceptable. While the term security guard is used by companies, government bodies and individuals, the term security officer is deemed more suitable. Bouncers use the title Crowd Controllers, and Store Detectives use the title Loss Prevention or Asset Protection Officers.

Security Officers may carry firearms, handcuffs or batons where their role requires them to do so and then only when working and have the appropriate sub-class accreditation to their license.

4.3.2 Canada

See also: Gun politics in Canada § Laws and regulation

In Canada, private security falls under the jurisdiction of Canada's ten provinces and three territories. All ten of Canada's provinces and one of its territories (the Yukon) have legislation that regulates the contract security industry.*[19] These eleven jurisdictions require that companies that provide security guard services and their employees be licensed.

Security vehicle and guard in Montreal, Quebec.

Most provinces in Canada regulate the use of handcuffs and weapons (such as firearms and batons) by contract security companies and their employees, either banning such use completely or permitting it only under certain circumstances. Additionally, in some provinces, some terms, or variations of them, are prohibited either on a uniform or in self-reference.*[20]

Canada's federal laws also restrict the ability of security guards to be armed. For example, section 17 of the Firearms Act makes it an offense for any person, including a security guard, to possess prohibited or restricted firearms (i.e. handguns) anywhere outside of his or her home.

There are two exceptions to this prohibition found in sections 18 and 19 of the Act. Section 18 deals with transportation of firearms while Section 19 deals with allowing persons to carry such firearms on their persons to protect their lives or the lives of other persons, or for the performance of their occupation (Armour Car Guards, Licensed Trappers), provided an Authorization to Carry (ATC) is first obtained.*[21]

British Columbia

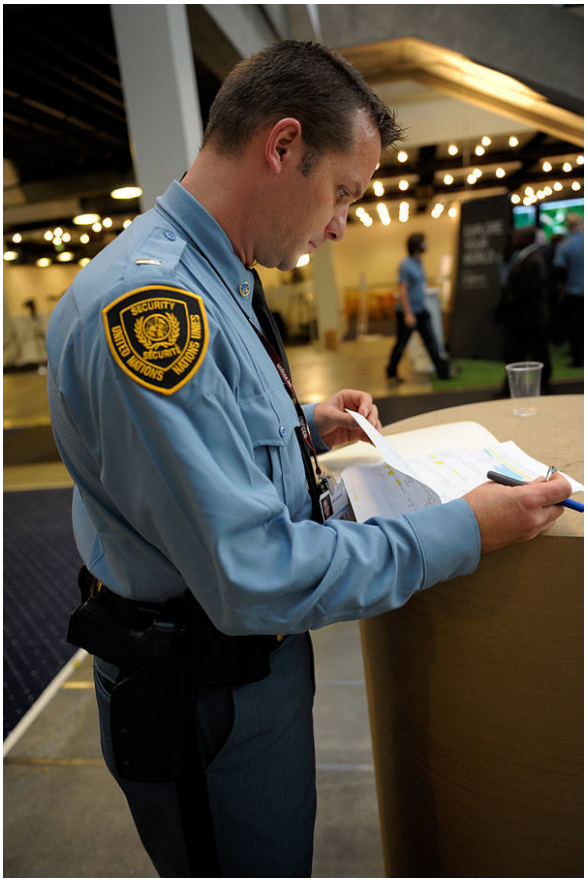
Private security in the province of British Columbia is governed by two pieces of legislation: the Security Services Act*[22] and the *Security Services Regulation*.*[23] These laws are administered and enforced by the Security Programs and Police Technology Division*[24] of the Ministry of Public Safety and Solicitor General.

The legislation requires that guards must be at least 19 years old, undergo a criminal background check, and successfully complete a training course.*[25] As far as weapons, British Columbia law severely restricts their use by security guards. Section 11(1)(c) of the Security Services Regulation prohibits security personnel from carrying or using any "item designed for debilitating or controlling a person or animal", which the government interprets to include all weapons. As well, section 11 forbids private security from using or carrying restraints, such as handcuffs, unless authorized by the government. However, as in other parts of Canada, armoured car guards are permitted to carry firearms.

In the past, only personnel that worked for contract security, that is, security companies, were regulated in British Columbia. However, as of September 1, 2009, in-house security guards and private investigators came under the jurisdiction of the Security Services Act and Security Services Regulation. Bodyguards and bouncers, effective November 1, 2009, are also subject to these regulations.*[26]

4.3.3 Europe

Armed private security are much rarer in Europe, and illegal in many countries, such as the United Kingdom, the Netherlands and Switzerland. In developing countries (with



A United Nations security officer at the 2009 United Nations Climate Change Conference in Copenhagen, Denmark.

host country permission), an armed security force composed mostly of ex-military personnel is often used to protect corporate assets, particularly in war-torn regions.

As a requirement of the Private Security Industry Act 2001, the UK now requires all contract security guards to have a valid Security Industry Authority license.* [27] The licence must be displayed when on duty, although a dispensation may be granted for store detectives, bodyguards and others who need to operate without being identified as a security guard. This dispensation is not available to Vehicle Immobilisers. Licenses are valid for three years and require the holders to undergo formal training, and are also to pass mandatory Criminal Records Bureau checks. Licences for Vehicle Immobilisers are valid for one year. Armed guarding and guarding with a weapon are illegal.

In Finland, all contract security guards are required to have a valid license granted by police. Temporary license is valid for four months and normal license for five years. License requires a minimum 40-hour course for temporary license and 60 hours more for a normal license. Additionally a narrow security vetting is required. The 40-hour course allows the carrying of a fixed-length baton and handcuffs, separate training and license is required for the security guard to carry pepper spray, extendable baton or a firearm. Rehearse of weapons usage is mandatory every year and is regulated by the Ministry of The Interior, to ensure the safe handling of pepper spray and such. Firearms can only be carried by bodyguards and cash-in-transit guards or when guarding a person or object that is significant in terms of public interest.* [28] In Finland, a security guard has the right to detain a person "red-handed", or seen committing a crime and the right to search the detained individual for harmful items and weapons. An individual who has been forcefully detained can only be released by the police. All companies providing security guarding services are also required to have a valid license from Suomen sisäministeriö (fi).* [29]

In the Netherlands, security guards (beveiligingsbeambte) must undergo a criminal background check by the local police department in the area where the private security company is located. To become a security guard in the Netherlands, a person must complete the basic training level 2 Beveiliger2. To complete the training a trainee must undergo a three-month internship with a private security company that is licensed by the svpb, the board that controls security exams. A trainee guard must pass for his diploma within one year. If the trainee does not pass he is not allowed to work anymore until he completes his training with a positive result. After a positive result a new ID can be issued and is valid for three years, after which the guard must undergo a background check by the local police again. Security guards in the Netherlands are not allowed to carry any kind of weapon or handcuffs. Every uniformed security guard in the Netherlands must have the V symbol on his or her uniform to advise the public they are dealing with a private guard; this rule is mandated by the Ministry of Justice. Security uniforms may not look like similar to police uniforms, and may not contain any kind of rank designation. The colors yellow and gold are not allowed to be used because the Dutch police uses gold accents in their uniforms; also, wearing a uniform cap is not longer allowed. Every new uniform design or addition must be approved by the Ministry of Justice before use. A patrol vehicle may not look like a police striped vehicle. The only private security guards who are allowed to carry firearms are those who work for the military or Dutch National bank (De Nederlandsche Bank); this is where the national gold reserve can be found.

Norway

In Norway security officers are called "Vektere". There are two different types of vektere—the normal uniformed or civil-clothing officers who watch over private and semi-public properties, and government-hired vektere who work

in public places, such as the Parliament. The law provides more enforcement powers to security officers in the Parliament than to private security officers.

Security officers must undergo three weeks of training and internship. They are allowed to work for six months after one week of the introduction course. It is also possible to choose Security as a high school major, which requires two years of school and two years of trainee positions at private companies, resulting in a certificate from the government. This certificate makes it easier to get a job, with slightly higher pay. It also makes it easier to get a job elsewhere in the security industry. The certificate can also be obtained by private security officers who have had a minimum of 5 years working experience.

No security officer may carry pepper spray, batons or any other kind of weapon. However, handcuffs may be used. Norges Bank (Bank of Norway, federal reserves) had armed goverment guards until late 2013, when they were disarmed by the minister of finance. Security officers serving on ships sailing in areas of high piracy risk may be equipped with firearms.

Uniforms should not resemble police worn attire, but some uniforms do. The uniform must have the text VEKTER or SIKKERHET above the left shirt pocket.

A security officer, or any other person, may detain or arrest anyone that violates any law, as long as the violation carries a punishment of mimimum six (6) months imprisonment and a fine. The detainee must be released or handed over to the authorities within 4 hours of the arrest.

Security officers assigned to public transportation, such as trains, subways, trams and buses, also have some powers under the Transportloven (transportation law). Security officers may issue fixed penalty tickets for violation of parking regulations in designated areas and for passengers on public transportation without a valid pass.

A security officer may only search (frisk) a person to prevent the use of or confiscate any type of weapon or anything that can be used as a weapon.

In 2006 some security officers (Vakt Service/Nokas) were given extended training and limited police authority to transport prisoners between police holding cells, jails and courts, etc. Due to an outcry from the police union, this program was scrapped after a few months.

In addition to normal "vektere" there also is a special branch for "Ordensvakter" who normally work as bouncers or security at concerts and similar types of events. Ordensvakter have to undergo an extra week of training to learn techniques on how to handle drunk people and people on various drugs. They also learn about the alcohol laws of Norway (which are rather strict). The police in the local police district must approve each Ordensvakt. These special regulations arose after events in the 1990s when bouncers had a bad reputation, especially in Oslo, for being too brutal and rough with people. At that time, the police had no control over who worked as bouncers. After the government implemented training and mandatory police-issued ID cards for bouncers the problems have been reduced. The police of Oslo report that Ordensvakter are now helping the police identify crimes that otherwise would not be reported.

In 2013, due to a high number of rapes and violent robberies, the city of Oslo (Oslo Kommune) hired a private security company (Metro Garda) to patrol the downtown immigrant areas. This patrol had a positive effect, and the city has, in addition to Metro Garda officers, now hired their own officers called Bymiljøetaten (City enviroment dep). The municipalities in Norway are not allowed to form their own "police". The only police force in Norway is the federal police (politi).

In 2007 several guards from the Securitas AB company were arrested for brutality against a robber they apprehended on the main street of Oslo. The crime was captured with a mobile camera by pedestrians and created a public outcry, with many objecting to the way the security guards took the law into their own hands. Later, it came to light that the thief first attacked the security guards when they approached him, so the brutality charges were dropped.*[30] As a result of this episode, the police said that they would be more careful when conducting criminal background checks for security guards. Before 2007 security guards were checked when they applied for a job, but not while they were working. Security companies were also criticized for not checking criminal records sufficiently, in some cases not at all. Now guards working in private security must be checked annually. The police have the authority to withdraw a company's licence if the company does not submit lists of employees to the police. The police in Norway were widely criticized for not checking guards properly, and even when they encounter an issue with a guard, the guard can still work for months before anything is done. The security company G4S, after being criticized by police for hiring criminals, stated that they cannot do anything about the problem, because only the police have the ability to check the guard's criminal records.*[31]

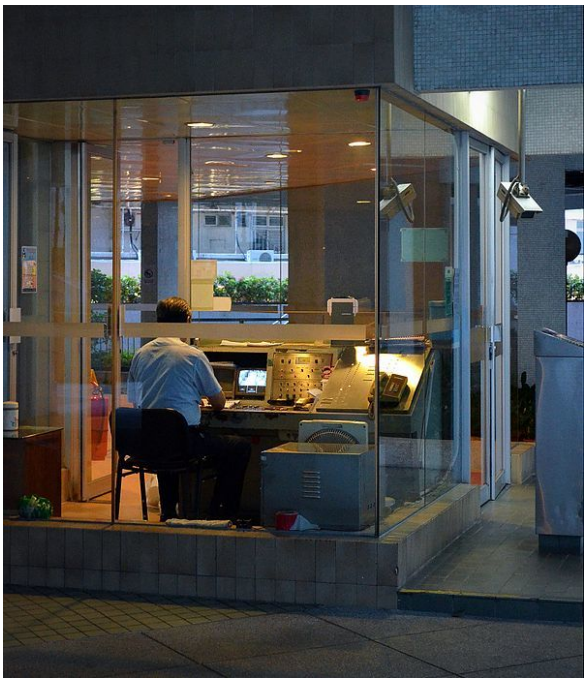
In 2012 Norwegian media reported that off-duty police officers and Home Guard soldiers had contracts of armed employment on civilian ships in the Aden bay, and police leaders were planning sanctions against the use of police officers.*[32]

Today there are around 15,000 people working in private security in Norway. The police have around 10,000 employees in total.

Notable companies operating in Norway:

- G4S
- Infratek
- ISS A/S (formerly Personellsikring)
- NOKAS
- ProSec—Professional Security (mainly event security)
- Securitas
- Metro Garda

4.3.4 Hong Kong



Watchman on duty at a residential block in Hong Kong.

In Hong Kong, the term *Security Officer* refers to a senior staff member who supervises a team of security personnel. The staff who work under security officers' supervision are called *Security Guards*.

Legislation

Before 1 October 1996, private security personnel were regulated by the *Watchmen Ordinance* (Chapter 299). However, there were many problems with that system of regulation—for example, there were no restrictions as to whom may establish private security service companies to provide security services to a client. Also, there was no regulation of people whom may perform installation of security systems.

Some employers hired "caretakers" instead of security guards to avoid their responsibilities under the ordinance (in formal definition, "caretakers" are supposed to provide facilities management service, although security service, which provided to residential properties, takes some parts of facilities management service). As a result, the Hong Kong Government enacted a wholly new law, the *Security and Guarding Services Ordinance* (Chapter 460), to replace the *Watchmen Ordinance*.

According to the *Security and Guarding Services Ordinance*: No individual shall do, agree to do, or hold himself/herself out as doing, or as available to do, security work for another person unless he/she does so-

- Under and in accordance with a permit; or
- Otherwise than for reward.*[33]

Security work means any of the following activities-

- Guarding any property;
- Guarding any person or place for the purpose of preventing or detecting the occurrence of any offence; (Replaced 25 of 2000 s. 2)
- Installing, maintaining or repairing a security device;
- Designing for any particular premises or place a system incorporating a security device.

Security device means a device designed or adapted to be installed in any premises or place, except on or in a vehicle, for the purpose of detecting or recording- (Amended 25 of 2000 s. 2)

- The occurrence of any offence; or
- The presence of an intruder or of an object that persons are, for reasons of security, not permitted to bring onto the premises or place or any other premises or place.*[34]

4.4 Qualification

Qualification for security guards vary from country to country. Different requirements have to be completed before applying for this job.

4.4.1 Hong Kong

Any applicant who wishes to apply for a Security Personnel Permit (SPP) must:

A group of Hong Kong security guards in formation before going on duty

- He/she have been living in Hong Kong for at least 5 years. (This requirement may have been changed)
- No criminal record.
- At least 17 years old when submitting his/her application.
- Have passed a mandatory 16 hour training course and have been granted a certificate of the course.
- If the applicant is over 65 years old, he/she must submit his/her health examination report.

Permit

Security Personnel Permit was separated to four types: A, B, C, and D.

- Type A permit holder was permitted to work in a "single-block" residential building; they are not allowed to carry firearms. No age limit.
- Type B permit holder was permitted to work in any type of properties, but they also are not allowed carry firearms. The maximum age limit of this permit is 65.
- Type C permit holder was permitted to work as an armed guard. (Usually, they are members of the cash transport car crew.) The maximum age limit of this permit is 55.
- Type D permit holder was permitted to design, install, and repair security devices. No maximum age limit.

The permit is valid for five years. All holders must renew their permit before it expires, or they will lose their qualification to work, as such, until their permit is renewed.

The type A and Type B security service are gradually combined with property management service, though the boundary between these two industries is unclear.

Power of Arrest

Security Guards in Hong Kong do not have special powers of arrest above that of the ordinary citizen, i.e. citizen's arrest, also known locally as the "101 arrest power". The Section 101 in the Criminal Procedure Ordinance addresses that arrest of an offender by a private citizen is allowed in certain circumstances if the offender is attempting an arrestable offense. Once arrested, the suspect must be delivered to a police office as soon as possible.

An arrestable offence is defined as any crime carrying a sentence of more than 12 months imprisonment. No security personnel are allowed to search other person, nor are they allowed to get personal information from other people, with the exception of some specific circumstances.

Security personnel at the Church of the Holy Sepulchre in Jerusalem.

4.4.2 Israel

In Israel, almost all security guards carry a firearm, primarily to prevent revenge attacks or terror attacks. Security guards are common: they perform entrance checks at shopping malls, transportation terminals, government and other office buildings, and many stores. Many locations with a high number of visitors, such as the Jerusalem Central Bus Station, employ X-ray machines to check passen-

ger's bags; in other places, they are opened and visually inspected. Since 2009, private security guards companies as Mikud have also replaced official security forces at some checkpoints inside and on the border of the West Bank, as well as the crossings to Gaza.

4.4.3 Malaysia

Peninsular Malaysia allows for the use of Nepalese security guards whereby East Malaysian immigration policy does not allow the use of foreign workers to be in employed in the security industry.

Security guard companies need to apply to the Ministry of Home Affairs (Kementerian Dalam Negeri).

Private security workers in Johannesburg during the 2010 World Cup.

4.4.4 South Africa

Main article: Private security industry in South Africa

Security guards along with the rest of the private security industry are regulated under Act 56 of 2001, Private Security Industry Regulation Act.*[35]

4.4.5 United States

Private security guards have outnumbered police officers since the 1980s, predating the heightened concern about security brought on by the September 11, 2001, attacks. The more than 1 million contract security officers, and an equal number of guards estimated to work directly for U.S. corporations, is much greater than the nearly 700,000 sworn law enforcement officers in the United States.*[36]

Most states require a license to work as a security officer.*[37] This license may include a criminal background check or mandated training requirements.

Security guards have the same powers of arrest as a private citizen, called a "private person" arrest, "any person" arrest, or "citizen's arrest". Most security officers do not carry weapons. If weapons are carried, additional permits and training are usually required. Armed security personnel are generally employed to protect sensitive sites such as government and military installations, armored money transports, casinos, banks and other financial institutions, and nuclear power plants. However, armed security is quickly becoming a standard for vehicle patrol officers and on many other non-government sites.

In some states, companies are developing technology to enhance private security. Using behavior analysis, computers can detect threats more quickly with fewer errors in judgement. Using specific algorithms, a computer can now detect aggressive and defensive body language, which triggers an alert to security or proper authorities depending on the event. These systems can also track slips and falls, theft and other events commonly experienced in corporate America.*[38]

The responsibilities of security guards in the United States are expanding in scope.*[2] For example, a trend is the increasing use of private security to support services previously provided by police departments. James F. Pastor addresses substantive legal and public policy issues which directly or indirectly relate to the provision of security services. These can be demonstrated by the logic of alternative or supplemental service providers. The use of private police has particular appeal because property or business owners can directly contract for public safety services, thereby providing welcome relief for municipal budgets. Finally, private police functions can be flexible, depending upon the financial, organizational, political, and circumstances of the client.*[39]

Arizona—Licensed security companies are required to provide eight hours of pre-assignment training to all persons employed as security guards before the employee acts in the capacity of a security guard.*[40] There is a state-mandated curriculum that must be taught, and subjects covered must include criminal law and laws of arrest, uniforms and grooming, communications, use of force, general security procedures, crime scene preservation, ethics, and first response.*[41]

California—Security Guards are required to obtain a license from the Bureau of Security and Investigative Services (BSIS), of the California Department of Consumer Affairs. Applicants must be at least 18 years old, undergo a criminal history background check through the California Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), and complete a 40-hour course of required training. This required training is broken down

An ADT Bel-Air Patrol vehicle

into smaller training sections and time-lines. The first is 8 hours of BSIS-designed instruction on powers to arrest and weapons. Then, within 30 days of getting the individual officers license, they must receive 16 hours of training on various mandatory and elective courses. Finally, within 6 months of getting their license, they must receive an additional 16 hours of training on various mandatory and elective courses.

California security officers are also required to complete 8 hours of annual training on security-related topics, in addition to the initial 40 hours of training.

The training and exam may be administered by any private patrol operator or by any of a large number of certified training facilities. This training can be in the classroom or online.*[42]*[43]

New Jersey—As of 2006 all security personnel must undergo a state mandated certified training program. This law, commonly referred to as SORA, is the state's effort to increase the quality of security personnel.

New Mexico—As of 2008 all security guards must undergo FBI background checks and a certified training program. Guards who carry firearms must also undergo additional training with a firearm through an approved firearms instructor and pass a psychological exam. The security industry is regulated through the New Mexico Regulation and Licensing Division.

North Carolina—Security Officers in North Carolina are required to register and become certified with the Private Protective Services Board (PPSB), the private security authority body under the North Carolina Department of Justice. The purpose of the Private Protective Services Board is to administer the licensing, education and training requirements for persons, firms, associations and corporations engaged in private protective services within North Carolina. The board is totally fee funded and is staffed by departmental employees directed on a daily basis by the Director, who is appointed by the Attorney General. There are two classifications for an officer: armed and unarmed. While an unarmed officer is required to take a 16 hour class of training and instruction to become certified, an armed officer must take additional hours of classroom training as well as qualify on a gun range with the firearm which will be carried on duty.

Oklahoma—Security officers in Oklahoma are licensed by CLEET (Council on Law Enforcement Education and Training). To be licensed as an unarmed officer an individual must be at least 18 years of age and undergo 40 hours of classroom training and pass criminal history checks. Armed guards must be 21 years of age, have another 40 hours of classroom training, qualify with their firearm and pass a psychological evaluation.

Oregon—Department of Public Safety, Standards and Training

Pennsylvania—No licensing requirements to be an unarmed security guard. However, anyone who carried a firearm or other "lethal weapon" in the course and scope of their employment must be trained as a "Certified Agent" and successfully complete a 40 hour training course (including shooting range time) in order to be certified to carry weapons while on duty under the Lethal Weapons Training Act (commonly referred to as Act 235 certification). Certification involves completing a medical physical exam, a psychological examination, classroom training and qualifying on a pistol range, with firing of 50 rounds of ammo larger than a .380acp. Agents are also required to qualify on a shotgun. The certification is good for five years at which time an eight hour refresher course must be taken or the certification is revoked. PA State Police—Lethal Weapons Training Program

South Carolina—All Security Officers have the same authority and power of arrest as Sheriff's Deputies, while on the property they are paid to protect, and according to Attorney General Alan Wilson, are considered Law Enforcement for the purpose of making arrests and swearing out a warrant before the magistrate.*[44] Private Officers may respond to calls for service, make arrests and use blue lights*[45] and traffic radar. They may also be specially authorized by the State Law Enforcement Division (SLED) to issue Uniform Traffic Tickets to violators.*[46] Security Officers are licensed or registered (as appropriate) by SLED for one year at a time. Training for unarmed officers is 8 hours, an additional 8 hours is required for a security weapons permit or a concealed security weapons permit. Additional hours are required to be documented for officers issuing public or private tickets as well as officers who will be using batons, pepper spray or tasers.

Virginia—Since the 1980s, Security Officers in Virginia

A museum guard in 1935.

are required to be certified by DCJS (Department of Criminal Justice Services, the same agency that certifies law enforcement officers).*[47] To be certified as an unarmed security officer one must go through 18 hours of classroom training from a certified instructor in order to obtain this card and it must be done by the end of their 90 days after hire with a Security company. Every two years the card must be renewed, by completing an in-service with a certified instructor. To be certified as an armed security officer one must complete an additional 24 hours of firearms training, 8 hours of training in conducting a lawful arrest, and qualification with the type and caliber of weapon they intend to carry. Firearms endorsements must be renewed annually by completing an in-service and passing a firearms qualification. Certified armed security officers are authorized under state code to arrest*[48] for any offense committed in their presence while they are on duty at the location they are hired to protect. Unarmed officers have no arrest powers. They also are granted the authority by the by state law to issue summons to appear in court*[49] for felonies and misdemeanors. Virginia also allows security officers to attend additional 40 hours of training to become certified as Conservators of the Peace (Special Police) for the company employing them. This appointment is performed by a Circuit Court Judge, wherein the officer is actually sworn in and has the powers of a police officer on property they are working, as well as the lawful duty to act upon witnessing any felony and the ability to pursue fleeing felons. Such sworn officers are also permitted the use of sirens and red lights. Those who handle K-9s, work as dispatchers, alarm responders, private investigators, instructors, bounty hunters, armored car couriers and Executive Protection Specialists are other categories of training regulated by DCJS with additional training requirements. All positions require State Police and FBI background checks.

St. Louis, Missouri—Security officers are required to be licensed by the St. Louis County Police Department or St. Louis Police Department. St. Louis County security officer training is a two-day class and yearly renewal class. Armed officers must shoot bi-annually to keep their armed status. County license is called a Metropolitan License, meaning it is good for St. Louis City and County.*[50] The St. Louis City web site has all the information regarding licensing requirements, as they are the same in the city and county.*[51]

4.5 Security officers and the police

Security personnel are not police officers, unless they are security police, but are often identified as such due to similar uniforms and behaviors, especially on private property. Security personnel in the U.S. derive their powers from state laws, which allow them a contractual arrangement with clients that give them Agent of the Owner powers.

This includes a nearly unlimited power to question with the absence of probable cause requirements that frequently dog public law enforcement officers.

Some jurisdictions do commission or deputize security officers and give them limited additional powers, particularly when employed in protecting public property such as mass transit stations. This is a special case that is often unique to a particular jurisdiction or locale. Additionally, security officers may also be called upon to act as an agent of law enforcement if a police officer, sheriff's deputy, etc. is in immediate need of help and has no available backup.

Some security officers do have reserve police powers and are typically employed directly by governmental agencies. Typically, these are sworn law enforcement personnel whose duties primarily involve the security of a government installation, and are also a special case.

Other local and state governments occasionally enter into special contracts with security agencies to provide patrol services in public areas. These personnel are sometimes referred to as "private police officers".

Sometimes, police officers work as security personnel while not on duty. This is usually done for extra income, and work is particularly done in hazardous jobs such as bodyguard work and bouncers outside nightclubs.

Police are called in when a situation warrants a higher degree of authority to act upon reported observations that security does not have the authority to act upon. However, some states allow Licensed Security Officers full ar-

rest powers equal to those of a Sheriff's Deputy.

In 1976, the Law Enforcement Assistance Administration's National Advisory Commission on Criminal Justice Standards and Goals reported:

> 'One massive resource, filled with significant numbers of personnel, armed with a wide array of technology, and directed by professionals who have spent their entire adult lifetimes learning how to prevent and reduce crime, has not been tapped by governments in the fight against criminality. The private security industry, with over one million workers, sophisticated alarm systems and perimeter safeguards, armored trucks, sophisticated mini-computers, and thousands of highly skilled crime prevention experts, offers a potential for coping with crime that can not be equalled by any other remedy or approach.... Underutilized by police, all but ignored by prosecutors and the judiciary, and unknown to corrections officials, the private security professional may be the only person in this society who has the knowledge to effectively prevent crime.'*[52]

In New York City, the Area Police/Private Security Liaison program was organized in 1986 by the NYPD commissioner and four former police chiefs working in the private security industry to promote mutual respect, cross-training, and sharing of crime-related information between public police and private security.

4.6 Trends

4.6.1 Australia

Private Security personnel initially outnumbered police. From the Australian Bureau of Statistics Report in 2006 there were 52,768 full-time security officers in the security industry compared to 44,898 police officers. But since Security Industry Regulation Act 2007 it has dropped to less than half that.

4.6.2 UK

The trend in the UK at the time of writing (March 2008) is one of polarisation. The market in Manned Guarding (the security industry term for the security guards most people are familiar with) is diverging toward two opposite extremes; one typified by a highly trained and well paid security officer; the other with security officers on or about minimum wage with only the minimum training required by law.

Within the "in-house" sector, where security personnel are not subject to licensing under the Private Security Industry Act 2001, the same divergence can be seen, with some companies opting for in-house security to maintain control of their standards, while others use it as a route to cheaper, non-regulated, security.

In a very few cases, such as the Northern Ireland Security Guard Service, security guards may be attested as Special Constables.

4.6.3 United States

Economist Robert B. Reich, in his 1991 book *The Work of Nations*, stated that in the United States, the number of private security guards and officers was comparable to the number of publicly paid police officers. He used this phenomenon as an example of the general withdrawal of the affluent from existing communities where governments provide public services. Instead, the wealthy pay to provide their own premium services, through voluntary, exclusive associations.

As taxpayer resistance has limited government budgets, and as the demand for secure homes in gated communities has grown, these trends have continued in the 1990s and 2000s (decade).

In the aftermath of the September 11, 2001 attacks, the trend in the US is one of a quiet transformation of the role of security guards into first responders in case of a terrorist attack or major disaster. This has resulted in longer guard instruction hours, extra training in terrorism tactics and increased laws governing private security companies in some states.*[53]

4.7 History

The *vigiles* were soldiers assigned to guard the city of Rome, often credited as the origin of both security personnel and police, although their principal duty was as a fire brigade. There have been night watchmen since at least the Middle Ages in Europe; walled cities of ancient times also had watchmen. A special chair appeared in Europe sometime in the late Middle Ages, called the watchman's chair; this unupholstered wooden chair had a forward slanting seat to prevent the watchman from dozing off during duty.

Standing Guard

4.8 Notable security guards

- Samuel Provance, known for his testimony regarding the abuse at Abu Ghraib prison, later became a Private Security Officer at a mall.
- The security guard Frank Wills detected the June 17, 1972 break-in at the Democratic National Committee headquarters at the Watergate office complex in Washington, D.C., ultimately leading to the resignation of Richard M. Nixon as President of the United States.
- Christoph Meili, night guard at a Swiss bank, became a whistle blower in 1997. He told about the bank destroying records related to funds of Holocaust victims, whose money the bank was supposed to return to their heirs.
- In 1999, Pierlucio Tinazzi rescued 10 victims from the Mont Blanc Tunnel Fire, before dying while trying to rescue an eleventh.
- In 2001, Gary Coleman, former child actor, was employed as a shopping mall security guard in the Los Angeles area. While shopping for a bullet-resistant vest for his job, Coleman assaulted a female autograph collector. Coleman said he felt "threatened by her insistence" and punched her in the head.*[54] He was later charged for the assault and ordered to pay her $1,665 for hospital bills.
- Derrick Brun, an unarmed security guard employed by the Red Lake School District in Minnesota, was praised by President Bush for his heroic role in protecting children during the 2005 Red Lake High School Massacre: "Derrick's bravery cost him his life, and all Americans honor him" .*[55]*[56]
- Armed security guard Jeanne Assam. In 2007, Matthew Murray fatally shot two and wounded two others at the Youth With A Mission retreat center in Arvada, Colorado. A few hours later he fatally shot two others and wounded another three in the New Life Church parking lot. When Murray entered the church, he was met by armed security guard Jeanne Assam, who ordered him to drop his weapon. Assam shot and wounded Murray when he failed to comply. The pastor of New Life Church credited Assam with saving over 100 lives.
- Richard Jewell, a security guard at Atlanta, Georgia's Centennial Olympic Park during the 1996 Summer Olympics who was wrongly accused of the Centennial Olympic Park bombing. Jewell was later cleared of those charges, and was in fact the one who saved hundreds of lives when he first noticed the suspicious package and got the area evacuated. Jewell later successfully sued several news agencies who reported him as the criminal prior to having the facts.

4.9 Unionization

4.9.1 Canada

Many security guards in Canada are unionized. The primary unions which represent security guards in Canada are the United Food and Commercial Workers (UFCW),*[57] Local 333, and the Canadian branch of the United Steelworkers (USW). In contrast to the legal restrictions in the United States, Canadian labour relations boards will certify bargaining units of security guards for a Canadian Labour Congress (CLC)-affiliated union or in the same union with other classifications of employees.

4.9.2 United States

In June 1947, the United States Congress passed the Taft-Hartley Act placing many restrictions on labor unions. Section 9 (B) (3) of the act prevents the National Labor Relations Board (NLRB) from certifying for collective bargaining any unit which mixes security employees with non-security employees. This restricts the ability of security employees to join any union that also represents other types of employees.

They may be part of an independent, "security-only" union, not affiliated with any coalition of other types of labor unions such as the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO). A union which also represents non-security employees may also represent and bargain on behalf of security employees with the employer's consent.

Two of the largest security unions are the Security, Police, and Fire Professionals of America (SPFPA) and the United Government Security Officers of America (UGSOA).

Security, Police, and Fire Professionals of America

In 1948 with the Taft-Hartley restrictions well into effect, the Detroit, Michigan area security guards of United Auto Workers (UAW) Amalgamated Local 114 were forced to break away and start a separate "Plant Guards Organizing Committee". The NLRB ruled that as an affiliate of the CIO, the committee was indirectly affiliated with production unions and therefore ineligible for certification under the new restrictions.

The committee was then forced to completely withdraw from the CIO and start the independent United Plant Guard Workers of America. By the 1990s, this union had evolved to include many other types of security officers and changed its name to the SPFPA.

United Government Security Officers of America

In 1992, the UGSOA was formed. It specializes in organizing federal, state, and local government security officers, but since May, 2000 has been open to representing other types of security personnel as well.

Others

The Service Employees International Union (SEIU) has also sought to represent security employees, although its efforts have been complicated by the Taft-Harley Act because the SEIU also represents janitors, trash collectors, and other building service employees.

4.10 Hazards in the Industry

Security personnel often are exposed to physical and physiological trauma that can have lasting effects. Security guards are at risk of being attacked by assailants. Other contributing factors are high workload, long hours, low pay, boredom and disregard of industry standards by employers and clients: e.g. break times, access to bathrooms and facilities, etc.

4.11 See also

4.12 References

[1] "Power to Arrest Training Manual - California Bureau of Security and Investigative Services" (PDF). Retrieved 2010-03-25.

[2] http://www.securityresources.net/Learn-How-to-Be-a-Licensed-Security-Guard.aspx

[3] "Bureau of Labor Statistics Occupational Outlook Handbook, 2008-09 Edition". Bls.gov. 2009-12-17. Retrieved 2010-03-25.

[4] "Morse Watchmans | Products | PowerCheck". Morsewatchman.com. Retrieved 2010-03-25.

[5] Kator, Zabi. "Supervisor accountabilites". *guardNOW*. guardNOW security services. Retrieved 1 May 2013.

[6] Kator, Zabi. "Scheduler". *guardNOW*. guardNOW Security Services. Retrieved 1 May 2013.

[7] Kator, Zabi. "Security Human Resources Manager". *website*. guardNOW Security Services. Retrieved 7 May 2013.

[8] Kator, Zabi. "Security Client Services Manager". *website*. guardNOW Security Services. Retrieved 7 May 2013.

[9] Kator, Zabi. "Security Client Services supervisor". *website*. guardNOW Security Services. Retrieved 7 May 2013.

[10] Rigakos, George (2002). *The New Parapolice: Risk Markets and the Commodification of Social Control*. Toronto: University of Toronto Press.

[11] McLeod, Ross (2004). *Parapolice: A Revolution in the Business of Law Enforcement*. Toronto: Boheme Press.

[12] Button, Mark (2007). *Security Officers and Policing: Powers, Culture and Control in the Governance of Private Space*. Aldershot publisher=Ashgate.com.

[13] "Private Security and Investigative Services Act, 2005, S.O. 2005, c. 34". E-laws.gov.on.ca. 2009-12-15. Retrieved 2010-03-25.

[14] http://www.assembly.ab.ca/bills/2008/pdf/bill-010.pdf

[15] Robertson, Brian (2008-05-28). "Province's Bill 10 makes "security officer" a punishable phrase". *Canadian Security* (CLB MEDIA INC). Retrieved 2008-06-05.

[16] "security guard services guide". Retrieved 2007-12-06.

[17] "City of Ceres, California, Chief de Werk's Weekly Article". Ci.ceres.ca.us. 2007-08-01. Retrieved 2010-03-25.

[18] http://www.oregon.gov/OSP/PATROL/docs/Law_Enforcement_Impersonators.pdf

[19] Government of Ontario, Canada. "Licences and Forms" . *Ministry of Community Safety and Correctional Services*. Government of Ontario. Retrieved 2007-09-03.

[20] Government of Ontario, Canada. "Licences and Forms" . *Ministry of Community Safety and Correctional Services*. Government of Ontario. Retrieved 2007-09-03.

[21] Government of Alberta, Canada. "Licences and Forms" . *Ministry of Community Safety and Correctional Services Alberta*. Government of Canada. Retrieved 2012-09-03.

[22] "Security Services Act" . Security Guards in Canada.

[23] "Security Services Regulation" . Government of British Columbia. Retrieved 2009-03-12.

[24] "Security Programs and Police Technology Division" . British Columbia Ministry of Public Safety and Solicitor General. Retrieved 2009-03-12.

[25] "JIBC | Police Academy | Security Training - BST1 BST2" . Jibc.ca. 2008-09-01. Retrieved 2010-03-25.

[26] "News and Updates" . British Columbia Ministry of Public Safety and Solicitor General. Retrieved 2009-06-29.

[27] "SIA website" . The-sia.org.uk. 2009-11-26. Retrieved 2010-03-25.

[28] "Private Security Services Act" . Retrieved 7 September 2014.

[29] "Ministry of the Interior unit for supervision of the private security industry" . Intermin.fi. Retrieved 2010-03-25.

[30] "Får ingen konsekvenser for vekterne" . dagbladet.no. Retrieved 2007-12-14.

[31] http://www.ringblad.no/jobb/article4876392.ece

[32] "Private sikkerheitsselskap leiger ut heimevernssoldatar og politimenn som væpna vakter på norske skip. Politiet planlegg sanksjonar, medan Heimevernet ikkje greier å stoppe tilstrøyminga" (in Norwegian). Klassekampen.no.

[33] "Security and Guarding Services Ordinance - Sect 10 Restrictions on doing security work" . Hklii.org. Retrieved 2010-03-25.

[34] "Security and Guarding Services Ordinance - Sect 2 Interpretation" . Hklii.org. 1997-06-30. Retrieved 2010-03-25.

[35] "Act 56 of 2001, Private Security Industry Regulation Act" . South African Government. Retrieved 2009-06-22.

[36] Goldstein, Amy (2010-08-23). "More security firms getting police powers / Some see benefits to public safety, but others are wary" . *The San Francisco Chronicle*.

[37] "Security Guards and Gaming Surveillance Officers" . Bls.gov. 2009-12-17. Retrieved 2010-03-25.

[38] http://www.amrelitech.com/amrelitech/DesktopDefault.aspx?tabindex=1&tabid=84

[39] Pastor, James F. (2003). *The Privatization of Police In America: An Analysis and Case Study*. Jefferson, NC: McFarland. ISBN 978-0-7864-1574-8.

[40] http://law.onecle.com/arizona/professions-and-occupations/32-2632.html

[41] http://licensing.azdps.gov/SGEightHourTrainingSyllabus.PDF

[42] "New Security Guard Training Regulation - Bureau of Security and Investigative Services" . Bsis.ca.gov. Retrieved 2010-03-25.

[43] "Security Guard Fact Sheet - Bureau of Security and Investigative Services" . Bsis.ca.gov. 2007-03-23. Retrieved 2010-03-25.

[44] South Carolina Code of Laws, Title 40,Chapter 18

[45] South Carolina Code of Laws, Title 56,Chapter 5 Section 170

[46] South Carolina, Attorney General's Opinion: Aug 01,1978 Apr 30, 1987 May 23, 1995 Aug 30, 2001 Oct 15, 2004 and State V. Brant (S.C.1982) 278 S.C. 188,293 SE2d 703

[47] "Legislative Information System" . Leg1.state.va.us. 2003-01-01. Retrieved 2010-03-25.

[48] "Legislative Information System" . Leg1.state.va.us. Retrieved 2010-03-25.

[49] "LIS > Code of Virginia > 19.2-74" . Leg1.state.va.us. Retrieved 2010-03-25.

[50] "Division of Operational Support Services". Stlouisco.com. 2001-09-11. Retrieved 2010-03-25.

[51] "SLMPD Private Security" . Slmpd.org. 2009-09-01. Retrieved 2010-03-25.

[52] National Advisory Commission on Criminal Justice Standards and Goals (NAC-CJSG) (1976). "Private Security: Report of the Task Force on Private Security" . Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration.

[53] "Contact Support" . Advancedsecurityguardservices.com. Retrieved 2010-03-25.

[54] "court TV becomes truTV". Courttv.com. Retrieved 2010-03-25.

[55] "President's Radio Address" . Georgewbush-whitehouse.archives.gov. 2005-03-26. Retrieved 2010-03-25.

[56] "Welcome to Serve.gov". Usafreedomcorps.gov. Retrieved 2010-03-25.

[57] About UFCW Canada

4.13 External links

- Ontario Ministry of Community Safety and Correctional Services information page on new private security legislation introduced in August, 2007
- UK private security industry legislation
- Small Arms Survey Research Note: Private Security Companies' Firearms Stockpiles

Chapter 5

Separation barrier

The Berlin Wall divided Berlin from 1961 until it was demolished in 1989

Green Line separation barrier, Cyprus

Separation barrier or **separation wall** is a barrier, wall or fence constructed to limit the movement of people across a certain line or border, or to separate peoples or cultures.*[1]

David Henley opines in The Guardian that separation barriers are being built at a record-rate around the world along borders and do not only surround dictatorships or pariah states. The term "separation barrier" has been applied to structures erected in Belfast, Homs, the West Bank, São Paulo, Cyprus, and along the Greece-Turkey border and the Mexico-United States border. Several erected separation barriers are no longer active or in place, including the Berlin Wall, the Maginot Line and some barrier sections in Jerusalem.*[2]

5.1 Cyprus

Since the Turkish invasion of Cyprus in 1974, Turkey has constructed and maintained what economics professor Rongxing Guo has called a "separation barrier" of 300 kilometres (190 mi) along the 1974 Green Line (or ceasefire line) dividing the island of Cyprus into two parts, with a United Nations buffer zone between them.*[3]

5.2 Egypt

The Egypt-Gaza barrier is often referred as "separation barrier" in the media.*[4] or as a "separating wall".*[5]*[6]*[7] In December 2009, Egypt started the construction of the Egypt–Gaza barrier along the Gaza border, consisting of a steel wall. Egypt's foreign minister said that the controversial wall, being built along the country's border with the Gaza Strip will defend it "against threats to national security".*[8] Though the construction paused a number of times, the wall is nearly complete.

5.3 Germany

Main article: Berlin Wall

5.4 Israel

Main article: West Bank security barrier

Israel has over the decades constructed several defensive barriers along its borders with surrounding nations, and has since 2002 constructed a substantial fortification to separate the country from the West Bank.*[9] following the failure of peace talks and a series of suicide bombings.

Palestinian protest art on separation barrier running through Bethlehem.

This barrier has caused much international controversy, because much of it is built outside of the 1949 Armistice Line. It cuts far into the West Bank and encompasses several of Israel's largest settlement blocs.

In June 2004, the Israeli Supreme Court ruled that building the wall on private Palestinian land is not in itself illegal, but ordered some changes to the original route, which separated 35,000 Palestinian farmers from their lands and crops. The Israeli finance minister replied at the time that it was disputed land, not Palestinian, and its final status would be resolved in negotiations.*[10] In July 2004, the International Court of Justice at The Hague, in a non-binding legal opinion, advised that the barrier was illegal under international law, and called on Israel to dismantle the barrier, return confiscated land and make reparations for damages.*[11]

Israel has said that the barriers are intended to prevent Palestinians from entering Israel to commit terrorist acts. The Palestinian government see them a means of confiscating West Bank land*[12] and of short-circuiting the peace process;*[10] former Palestinian Authority leader Yasser Arafat stated that their goal was to prevent the establishment of a Palestinian state.

5.5 Kuwait

Writer Damon DiMarco has described as a "separation barrier" the Kuwait-Iraq barricade constructed by the United Nations in 1991 after the Iraqi invasion of Kuwait was repelled. With electrified fencing and concertina wire, it includes a 15-foot-wide trench and a high berm. It runs 120 miles along the border between the two nations.*[13]

5.6 Malaysia

Renee Pirrong of the Heritage Foundation described the Malaysia–Thailand border barrier as a "separation barrier." Its purpose is to cut down on smuggling, drug trafficking, illegal immigration, crime and insurgency.*[14]

5.7 Saudi Arabia

In 2004 Saudi Arabia began construction of a Saudi-Yemen barrier between its territory and Yemen to prevent the unauthorized movement of people and goods into and out of the Kingdom. Some have labeled it a "separation barrier." *[15] In February 2004 The Guardian reported that Yemeni opposition newspapers likened the barrier to the Israeli West Bank barrier,*[16] while *The Independent* wrote "Saudi Arabia, one of the most vocal critics in the Arab world of Israel's 'security fence' in the West Bank, is quietly emulating the Israeli example by erecting a barrier along its porous border with Yemen" .*[17] Saudi officials rejected the comparison saying it was built to prevent infiltration and smuggling.*[16]

5.8 Slovakia

BBC reporter Nick Thorpe described a 150-meter-long and 2.2-meter-high wall in the Slovakian town of Ostrovany as a "separation barrier" and compares it to the Berlin Wall and the Israeli separation barriers because it is meant to divide the two-thirds majority Roma population from the native Slovaks. Slovaks accuse the Roma of stealing their fruit, vegetables and metal fence posts.*[18]

5.9 United Kingdom

Main article: Peace lines

Over 21 miles of high walling or fencing separate Catholic and Protestant communities in Northern Ireland, with most concentrated in Belfast and Derry/Londonderry. The wall was built in 1969 in order to separate the Catholic and Protestant areas in Belfast.*[19] An Army Major, overseeing the construction of the wall at the time, said: 'This is a temporary measure ···we do not want to see another Berlin wall situation in Western Europe ···it will be gone by Christmas'. In 2013, that wall still remains and almost 100 additional walls and barriers now complement the original. Technically known as 'peace walls', there are moves to remove all of them by 2023 by mutual consent.*[20]

5.10 United States

Beach in Tijuana at the American-Mexican border, circa 2006

The United States has constructed a barrier along 130 kilometres (81 mi) of its border with Mexico of 3,169 kilometres (1,969 mi) to prevent unauthorized immigration into the United States and to deter smuggling of contraband. The Georgetown Journal of Law has referred to it as a "separation barrier" and suggests that while it is "revolting to many as an ugly face of separation" it could be used as an opportunity if part of a larger program of "foreign aid, infrastructure investment and regional development." *[21]

5.11 See also

- Defensive walls
- List of fortifications
- List of walls
- List of cities with defensive walls
- Buffer zone

5.12 References

[1] "The fence along the Mexican-U.S. border is just one of many barriers proposed or constructed around the world to keep people and cultures separated. Learn more about them below."

[2] David Henley, Walls: an illusion of security from Berlin to the West Bank, The Guardian, November 19, 2013.

[3] Rongxing Guo, *Territorial Disputes and Resource Management: A Global Handbook*, Nova Publishers, 2006, p 91, ISBN 1600214452, 9781600214455

[4] "Egypt-Gaza Border Quiet Despite Political Rhetoric - Al-Monitor: the Pulse of the Middle East". Al-Monitor. Retrieved 2013-11-22.

[5] Fleishman, Jeffrey; Hassan, Amro (2009-12-21). "Egypt's barrier along Gaza border called 'wall of shame' - Los Angeles Times". Articles.latimes.com. Retrieved 2013-11-22.

[6] Younis, Nora; Knickmeyer, Ellen (2008-01-26). "'Dear Palestinian Brothers . . . Please Return to Gaza'". Washingtonpost.com. Retrieved 2013-11-22.

[7] Erlanger, Steven (2008-01-26). "Egypt Tries to Plug Border; Gazans Poke New Hole". *The New York Times*. Retrieved 2013-11-22.

[8] "Egypt defends Gaza wall - Middle East". Al Jazeera English. Retrieved 2013-11-22.

[9] Steven Poole, *Unspeak: How Words Become Weapons, How Weapons Become a Message, and How That Message Becomes Reality*, Grove Press, 2007, p. 78-83, ISBN 0802143059, 9780802143051

[10] "USATODAY.com - Israel orders separation barrier changes". Usatoday30.usatoday.com. 2004-06-30. Retrieved 2013-11-22.

[11] "U.N. court rules West Bank barrier illegal - Jul 9, 2004". CNN.com. 2004-07-10. Retrieved 2013-11-22.

[12] "Thousands march in protest against separation barrier - SpecialsMiddleEastConflict". www.smh.com.au. 2004-02-24. Retrieved 2013-11-22.

[13] Damon DiMarco, *Heart of War: Soldiers? Voices*, Citadel Press, 2007, p. 129, ISBN 0806528141, 9780806528144

[14] Renee Pirron, http://blog.heritage.org/2010/08/06/fences-and-neighbors/, Heritage Foundation blog, August 6, 2010

[15] Anthony H. Cordesman, *Saudi Arabia: National Security in a Troubled Region*, p. 276.

[16] Whitaker, Brian (February 17, 2004). "Saudi security barrier stirs anger in Yemen". London: The Guardian. Retrieved 2007-03-23.

[17] Bradley, John (February 11, 2004). "Saudi Arabia enrages Yemen with fence". London: The Independent. Retrieved 2007-03-23.

[18] Nick Thorpe, Slovakia's separation barrier to keep out Roma , BBC, March 9, 2010.

[19] "The wall was built in 1969 to separate the Catholic Falls Road and the Protestant Shankill Road. An Army Major, overseeing the construction of the wall at the time, said: 'This is a temporary measure ⋯we do not want to see another Berlin wall situation in Western Europe ⋯it will be gone by Christmas'. In 2013, that wall still remains and almost 100 additional walls and barriers now complement the original. "

[20] "Robinson and McGuinness want "peace walls"down within 10 years". *The Irish Times*. 10 May 2013. Retrieved 5 January 2014.

[21] The Georgetown Journal of Law & Public Policy, Volume 5, Georgetown University Law Center, 2007, p. 347.

5.13 External links

- Security Fences around the World
- Security Fences in *The Atlantic Monthly*
- Article about CityWalls on Erasmuspc
- "Obama's Border Fence", NOW on PBS, July 3, 2009.

Chapter 6

Lock (security device)

"Lock and key" redirects here. For the novel by Sarah Dessen, see Lock and Key.

A **lock** is a mechanical or electronic fastening device that is released by a physical object (such as a key, keycard, fingerprint, RFID card, security token etc.), by supplying secret information (such as a keycode or password), or by a combination thereof.

Locks

6.1 History

6.1.1 Antiquity

Medieval lock in Kathmandu

The earliest known lock and key device was discovered in the ruins of Nineveh, the capital of ancient Assyria.*[1] Locks such as this were later developed into the Egyptian wooden pin lock, which consisted of a bolt, door fixture, and key. When the key was inserted, pins within the fixture were lifted out of drilled holes within the bolt, allowing it to move. When the key was removed, the pins fell part-way into the bolt, preventing movement.*[2]

The warded lock was also present from antiquity and remains the most recognizable lock and key design in the Western world. The first all-metal locks appeared between the years 870 and 900, and are attributed to the English craftsmen.*[3] It is also said that the key was invented by Theodore of Samos in the 6th century BC.*[4]

Affluent Romans often kept their valuables in secure boxes within their households, and wore the keys as rings on their fingers. The practice had two benefits: It kept the key handy at all times, while signaling that the wearer was wealthy and important enough to have money and jewelry worth secur-

Simple three-disc locking mechanism from a wooden box recovered from the Swedish ship Vasa, sunk in 1628

ing.*[5]

6.1.2 Modern locks

Chinese lock and key from Yunnan Province, early 20th century

With the onset of the Industrial Revolution in the late 18th century and the concomitant development of precision engineering and component standardisation, locks and keys were manufactured with increasing complexity and sophistication.

The lever tumbler lock, which uses a set of levers to prevent the bolt from moving in the lock, was perfected by Robert Barron in 1778. His double acting lever lock required the lever to be lifted to a certain height by having a slot cut in the lever, so lifting the lever too far was as bad as not lifting the lever far enough. This type of lock is still currently used today.*[6]

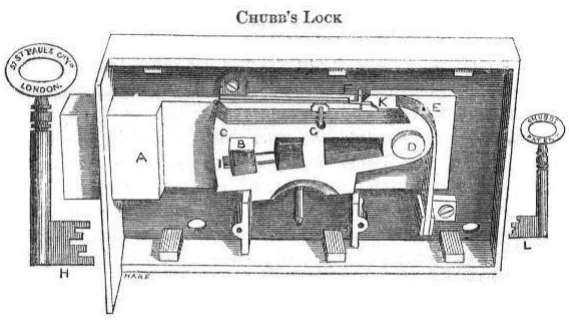


Diagram of a Chubb detector lock

The lever tumbler lock was greatly improved by Jeremiah Chubb in 1818. A burglary in Portsmouth Dockyard prompted the British Government to announce a competition to produce a lock that could be opened only with its own key.*[7] Chubb developed the Chubb detector lock, which incorporated an integral security feature that could frustrate unauthorised access attempts and would indicate to the lock's owner if it had been interfered with. Chubb was awarded £100 after a trained lock-picker failed to break the lock after 3 months.*[8]

In 1820, Jeremiah joined his brother Charles in starting their own lock company, Chubb. Chubb made various improvements to his lock; - his 1824 improved design didn't require a special regulator key to reset the lock, by 1847 his keys used six-levers rather than four and he later introduced a disc that allowed the key to pass but narrowed the field of view, hiding the levers from anybody attempting to pick the lock.*[9] The Chubb brothers also received a patent for the first burglar-resisting safe and began production in 1835.

The designs of Barron and Chubb were based on the use of movable levers, but Joseph Bramah, a prolific inventor, developed an alternative method in 1784. His lock used a cylindrical key with precise notches along the surface; these moved the metal slides that impeded the turning of the bolt into an exact alignment, allowing the lock to open. The lock was at the limits of the precision manufacturing capabilities of the time and was said by its inventor to be unpickable. In the same year Bramah started the Bramah Locks company at 124 Piccadilly, and displayed the "Challenge Lock" in the window of his shop from 1790, challenging "...the artist who can make an instrument that will pick or open this lock" for the reward of £200. The challenge stood for over 67 years until, at the Great Exhibition of 1851, the American locksmith Alfred Charles Hobbs was able to open the lock and, following some argument about the circumstances under which he had opened it, was awarded the prize. Hobbs' attempt required some 51 hours, spread over 16 days.

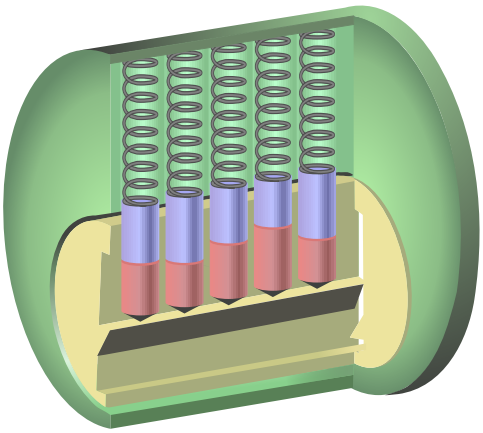
The earliest patent for a double-acting pin tumbler lock

was granted to American physician Abraham O. Stansbury in England in 1805,*[10] but the modern version, still in use today, was invented by American Linus Yale, Sr. in 1848.*[11] This lock design used pins of varying lengths to prevent the lock from opening without the correct key. In 1861, Linus Yale, Jr. was inspired by the original 1840s pin-tumbler lock designed by his father, thus inventing and patenting a smaller flat key with serrated edges as well as pins of varying lengths within the lock itself, the same design of the pin-tumbler lock which still remains in use today.*[12] The modern Yale lock is essentially a more developed version of the Egyptian lock.

Despite some improvement in key design since, the majority of locks today are still variants of the designs invented by Bramah, Chubb and Yale.

6.2 Types of locks

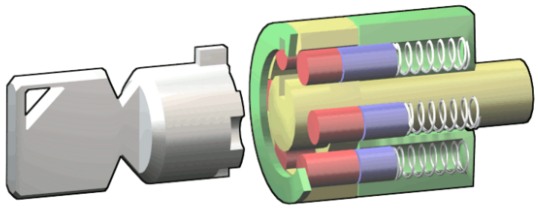
6.2.1 Locks with physical keys



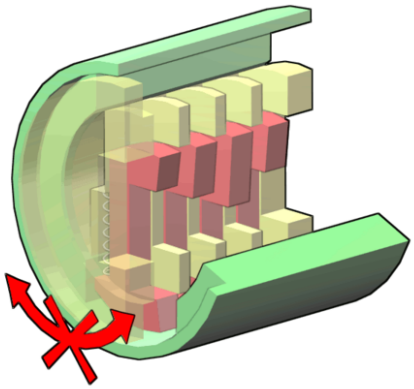
Pin tumbler lock: without a key in the lock, the driver pins (blue) are pushed downwards, preventing the plug (yellow) from rotating

A **warded lock** uses a set of obstructions, or wards, to prevent the lock from opening unless the correct key is inserted. The key has notches or slots that correspond to the obstructions in the lock, allowing it to rotate freely inside the lock. Warded locks are typically reserved for low-security applications as a well-designed skeleton key can successfully open a wide variety of warded locks.

The **pin tumbler lock** uses a set of pins to prevent the lock from opening unless the correct key is inserted. The key has a series of grooves on either side of the key's blade that limit the type of lock the key can slide into. As the key slides into the lock, the horizontal grooves on the blade align



Tubular lock: the key pins (red) and driver pins (blue) are pushed towards the front of the lock, preventing the plug (yellow) from rotating. The tubular key has several half-cylinder indentations which align with the pins



Wafer tumbler lock: without a key in the lock, the wafers (red) are pushed down by springs. The wafers nestle into a groove in the lower part of the outer cylinder (green) preventing the plug (yellow) from rotating

with the wards in the keyway allowing or denying entry to the cylinder. A series of pointed teeth and notches on the blade, called bittings, then allow pins to move up and down until they are in line with the shear line of the inner and outer cylinder, allowing the cylinder or cam to rotate freely and the lock to open.

A **wafer tumbler lock** is similar to the pin tumbler lock and works on a similar principle. However, unlike the pin lock (where each pin consists of two or more pieces) each wafer is a single piece. The wafer tumbler lock is often incorrectly referred to as a disc tumbler lock, which uses an entirely different mechanism. The wafer lock is relatively inexpensive to produce and is often used in automobiles and cabinetry.

The **disc tumbler lock** or **Abloy lock** is composed of slotted rotating detainer discs. They are considered very secure and almost impossible to pick.

The **lever tumbler lock** uses a set of levers to prevent the bolt from moving in the lock. In its simplest form, lifting

the tumbler above a certain height will allow the bolt to slide past.

6.2.2 Locks with electronic keys

An electronic lock works by means of an electronic current and is usually connected to an access control system. In addition to the pin and tumbler used in standard locks, electronic locks connects the bolt or cylinder to a motor within the door using a part called an actuator Types of electronic locks include the following:

A keycard lock operates with a flat card using the same dimensions as a credit card or US and EU drivers license. In order to open the door, one needs to successfully match the signature within the **keycard**.

A **Smart Lock** is an electromechanics lock that gets instructions to lock and unclock the door from an authorized device using a cryptographic key and wireless protocol. **smart locks** have begun to be used more commonly in residential areas, and have most likely grown in popularity due to widespread use of the smartphone.*[13]

6.2.3 List of common locks

- Bicycle lock
- Cam lock
- Chamber lock
- Child safety lock
- Combination lock
- Cylinder lock
- Deadbolt
- Electronic lock
- Electric strike
- Magnetic lock
- Mortise lock
- Lever tumbler lock
- Chubb detector lock
- Police lock
- Protector lock
- Luggage lock
- Magnetic keyed lock
- Padlock
- RFID
- Rim lock
- Time lock

6.3 Locksmithing

Locksmith, 1451

Locksmithing is a traditional trade, and in most countries requires completion of an apprenticeship. The level of formal education required varies from country to country, from a simple training certificate awarded by an employer, to a full diploma from an engineering college. Locksmiths may be commercial (working out of a storefront), mobile (working out of a vehicle), institutional, or investigational (forensic locksmiths). They may specialize in one aspect of the skill, such as an automotive lock specialist, a master key system specialist or a safe technician. Many also act as security consultants, but not all security consultants have the skills and knowledge of a locksmith.

Historically, locksmiths constructed or repaired an entire lock, including its constituent parts. The rise of cheap mass production has made this less common; the vast majority of

locks are repaired through like-for-like replacements, high-security safes and strongboxes being the most common exception. Many locksmiths also work on any existing door hardware, including door closers, hinges, electric strikes, and frame repairs, or service electronic locks by making keys for transponder-equipped vehicles and implementing access control systems.

Although the fitting and replacement of keys remains an important part of locksmithing, modern locksmiths are primarily involved in the installation of high quality lock-sets and the design, implementation, and management of keying and key control systems. A locksmith is frequently required to determine the level of risk to an individual or institution and then recommend and implement appropriate combinations of equipment and policies to create a "security layer" that exceeds the reasonable gain of an intruder.

In the United States, the locksmith industry exhibited steady growth in the years following 2010. In 2012, total revenue was over $1.6 billion with more than 3,600 locksmiths in operation.*[14]

6.3.1 Full disclosure

Full disclosure requires that full details of a security vulnerability are disclosed to the public, including details of the vulnerability and how to detect and exploit it. The theory behind *full disclosure* is that releasing vulnerability information immediately results in better security. Fixes are produced faster because vendors and authors are forced to respond in order to protect their system from potential attacks as well as to protect their own image. Security is improved because the *window of exposure*, the amount of time the vulnerability is open to attack, is reduced. The issue of full disclosure was first raised in a 19th-century controversy over the revelation of lock-system weaknesses to the public. According to A. C. Hobbs:

> A commercial, and in some respects a social doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done. If a lock, let it have been made in whatever country, or by whatever maker, is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically;and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.
>
> It cannot be too earnestly urged that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give instructions in the art of adulterating milk; a vain fear, milkmen knew all about it before, whether they practiced it or not; and the exposure only taught purchasers the necessity of a little scrutiny and caution, leaving them to obey this necessity or not, as they pleased.
>
> —A. C. Hobbs (Charles Tomlinson, ed.), *Locks and Safes: The Construction of Locks.* Published by Virtue & Co., London, 1853 (revised 1868).

6.3.2 Famous locksmiths

- Robert Barron patented a double-acting tumbler lock in 1778, the first reasonable improvement in lock security.
- Joseph Bramah patented the Bramah lock in 1784.*[15] It was considered unpickable for 67 years until A.C. Hobbs picked it, taking over 50 hours.*[16]
- Jeremiah Chubb patented his detector lock in 1818. It won him the reward offered by the Government for a lock that could not be opened by any but its own key.
- James Sargent described the first successful key-changeable combination lock in 1857. His lock became popular with safe manufacturers and the United States Treasury Department. In 1873, he patented a time lock mechanism, the prototype for those used in contemporary bank vaults.
- Samuel Segal of the Segal Lock and Hardware Company invented the first jimmy-proof locks in 1916.
- Harry Soref founded the Master Lock Company in 1921 and patented an improved padlock in 1924 with a patent lock casing constructed out of laminated steel.
- Linus Yale, Sr. invented a pin tumbler lock in 1848.
- Linus Yale, Jr. improved upon his father's lock in 1861, using a smaller, flat key with serrated edges that

is the basis of modern pin-tumbler locks. Yale developed the modern combination lock in 1862.

6.4 See also

- Access control
- Associated Locksmiths of America
- Door security
- Industrial revolution
- Exit control lock
- Master Locksmiths Association
- Physical security
- Rope lock
- Security door chain

6.5 References

[1] de Vries, N. Cross and D. P. Grant, M. J. (1992). *Design Methodology and Relationships with Science: Introduction*. Eindhoven: Kluwer Academic Publishers. p. 32.

[2] Ceccarelli, Marco (2004). *International Symposium on History of Machines and Mechanisms*. New York: Kluwer Academic Publishers. p. 43. ISBN 1402022034.

[3] "History". Locks.ru. Retrieved 2010-06-10.

[4] "History". Dimensions Info. Retrieved 2012-12-09.

[5] "History". Slate Magazine. Retrieved 2012-12-09.

[6] Pulford, Graham W. (2007). *High-Security Mechanical Locks : An Encyclopedic Reference*. Elsevier. p. 317. ISBN 0-7506-8437-2.

[7] "History of Locks". *Encyclopaedia of Locks and Builders Hardware*. Chubb Locks. 1958. Retrieved 16 November 2006.

[8] "Lock Making: Chubb & Son's Lock & Safe Co Ltd". Wolverhampton City Council. 2005. Retrieved 16 November 2006.

[9] Roper, C.A.; & Phillips, Bill (2001). *The Complete Book of Locks and Locksmithing*. McGraw-Hill Publishing. ISBN 0-07-137494-9.

[10] *The Complete Book of Home, Site, and Office Security: Selecting, Installing, and Troubleshooting Systems and Devices*. McGraw-Hill Professional. p. 11.

[11] *The Geek Atlas: 128 Places Where Science and Technology Come Alive*. O'Reilly Media, Inc. p. 445.

[12] "Inventor of the Week Archive". Massachusetts Institute of Technology.

[13] , Ditch the Keys: It's Time to Get a Smart Lock, Popular Mechanics .

[14] "Locksmith Market Research Report". Pell Research.

[15] "Opening an Antique Bramah Box Lock". Hygra.com. Retrieved 2012-08-15.

[16] "Bramah Locks". Crypto.com. Retrieved 2012-08-15.

6.6 Further reading

- Phillips, Bill. (2005). *The Complete Book of Locks and Locksmithing*. McGraw-Hill. ISBN 0-07-144829-2.
- Alth, Max (1972). *All About Locks and Locksmithing*. Penguin. ISBN 0-8015-0151-2
- Robinson, Robert L. (1973). *Complete Course in Professional Locksmithing* Nelson-Hall. ISBN 0-911012-15-X

6.7 External links

- Lockwiki
- "Historical locks" by Raine Borg and ASSA ABLOY
- "Picking Locks", *Popular Mechanics*

Chapter 7

Access control

For access control on a highway, see controlled-access highway. For standardized forms of names in a library catalog, see authority control.

In the fields of physical security and information security, **access control** is the selective restriction of access to a place or other resource.[*][1] The act of *accessing* may mean consuming, entering, or using. Permission to access a resource is called *authorization*.

A soldier allows a driver to enter a military base.

Locks and login credentials are two analogous mechanisms of access control.

Underground entrance to the New York City Subway system

7.1 Physical security

Main article: Physical security

Geographical access control may be enforced by personnel (e.g., border guard, bouncer, ticket checker), or with a device such as a turnstile. There may be fences to avoid circumventing this access control. An alternative of access control in the strict sense (physically controlling access itself) is a system of checking authorized presence, see e.g. Ticket controller (transportation). A variant is exit control, e.g. of a shop (checkout) or a country.

The term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access control is a matter of who, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically, this was partially accomplished through keys and locks. When a door is locked, only someone with a key can enter through the door, depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door, and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.

Physical security access control with a hand geometry scanner

Example of fob based access control using an ACT reader

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

7.1.1 Access control system operation

When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room, but Bob does not. Alice either gives Bob her credential, or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.

There are three types (factors) of authenticating information:[*] [2]

- something the user knows, e.g. a password, passphrase or PIN
- something the user has, such as smart card or a key fob
- something the user is, such as fingerprint, verified by biometric measurement

Passwords are a common means of verifying a user's identity before access is given to information systems. In addition, a fourth factor of authentication is now recognized: someone you know, whereby another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios. For example, a user may have their password, but have forgotten their smart card. In such a scenario, if

the user is known to designated cohorts, the cohorts may provide their smart card and password, in combination with the extant factor of the user in question, and thus provide two factors for the user with the missing credential, giving three factors overall to allow access.

7.1.2 Credential

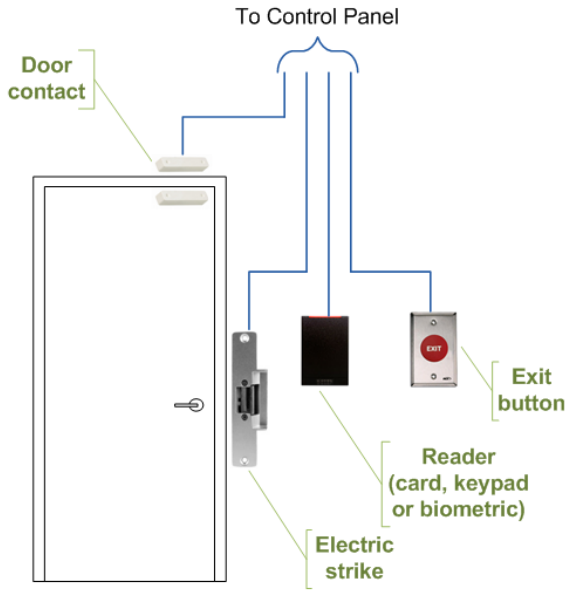
A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something a person knows (such as a number or PIN), something they have (such as an access badge), something they are (such as a biometric feature) or some combination of these items. This is known as multi-factor authentication. The typical credential is an access card or key-fob, and newer software can also turn users' smartphones into access devices.*[3] There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26-bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs, which are more compact than ID cards, and attach to a key ring. Biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry.*[4] The built-in biometric technologies found on newer smartphones can also be used as credentials in conjunction with access software running on mobile devices.*[5] In addition to older more traditional card access technologies, newer technologies such as Near field communication (NFC) and Bluetooth low energy also have potential to communicate user credentials to readers for system or building access.*[6]*[7]

7.1.3 Access control system components

control system components can be found in major cities such as New York City

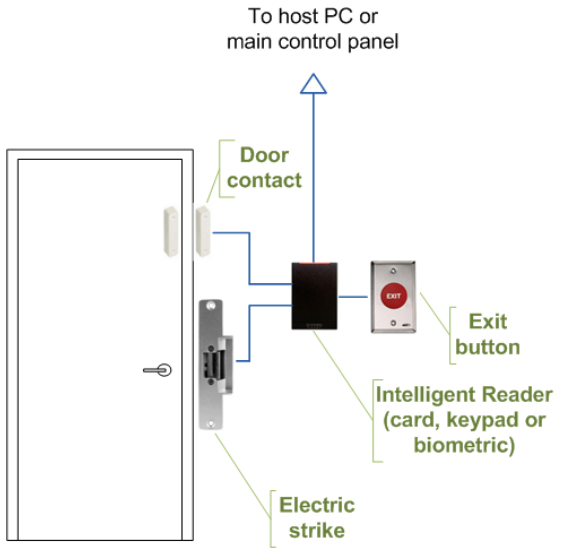
An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier, where granting access can be electronically controlled. Typically, the access point is a door. An electronic access control door can contain several elements. At its most basic, there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision, but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch can be used. In concept, the door switch is not unlike those on refrigerators or car doors. Generally only entry is controlled, and exit is uncontrolled. In cases where exit is also controlled, a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (REX) is used. Request-to-exit devices can be a push-button or a motion detector. When the button is pushed, or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

7.1.4 Access control topology



Typical access control door wiring

Access control decisions are made by comparing the credential to an access control list. This look-up can be done by a host or server, by an access control panel, or by a



Access control door wiring when using intelligent readers

reader. The development of access control systems has seen a steady push of the look-up out from a central host to the edge of the system, or the reader. The predominant topology circa 2009 is hub and spoke with a control panel as the hub, and the readers as the spokes. The look-up and control functions are by the control panel. The spokes communicate through a serial connection; usually RS-485. Some manufactures are pushing the decision making to the edge by placing a controller at the door. The controllers are IP enabled, and connect to a host and database using standard networks.

7.1.5 Types of readers

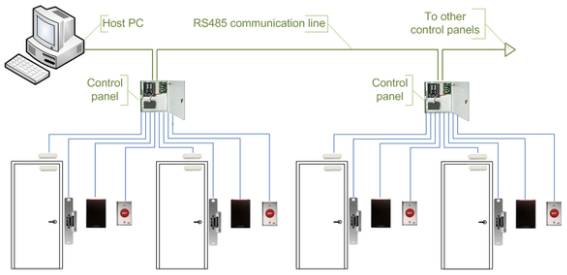
Access control readers may be classified by the functions they are able to perform:

- Basic (non-intelligent) readers: simply read card number or PIN, and forward it to a control panel. In case of biometric identification, such readers output the ID number of a user. Typically, Wiegand protocol is used for transmitting data to the control panel, but other options such as RS-232, RS-485 and Clock/Data are not uncommon. This is the most popular type of access control readers. Examples of such readers are RF Tiny by RFLOGICS, ProxPoint by HID, and P300 by Farpointe Data.
- Semi-intelligent readers: have all inputs and outputs necessary to control door hardware (lock, door contact, exit button), but do not make any access decisions. When a user presents a card or enters a PIN, the reader sends information to the main controller, and waits for its response. If the connection to the main controller is interrupted, such readers stop working, or function in a degraded mode. Usually semi-intelligent readers are connected to a control panel via an RS-485 bus. Examples of such readers are InfoProx Lite IPL200 by CEM Systems, and AP-510 by Apollo.
- Intelligent readers: have all inputs and outputs necessary to control door hardware; they also have memory and processing power necessary to make access decisions independently. Like semi-intelligent readers, they are connected to a control panel via an RS-485 bus. The control panel sends configuration updates, and retrieves events from the readers. Examples of such readers could be InfoProx IPO200 by CEM Systems, and AP-500 by Apollo. There is also a new generation of intelligent readers referred to as "IP readers". Systems with IP readers usually do not have traditional control panels, and readers communicate directly to a PC that acts as a host. Examples of such readers are Foxtech FX-50UX, FX-632 Fingerprint Reader/Controller Access Control System PowerNet IP Reader byIsonas Security Systems,* [8] ID 11 by Solus (has a built in webservice to make it user friendly), Edge ER40 reader by HID Global, LogLock and UNiLOCK by ASPiSYS Ltd, BioEntry Plus reader by Suprema Inc., and 4G V-Station by Bioscrypt Inc.

Some readers may have additional features such as an LCD and function buttons for data collection purposes (i.e. clock-in/clock-out events for attendance reports), camera/speaker/microphone for intercom, and smart card read/write support.

Access control readers may also be classified by their type of identification technology.

7.1.6 Access control system topologies



Access control system using serial controllers

1. **Serial controllers.** Controllers are connected to a host

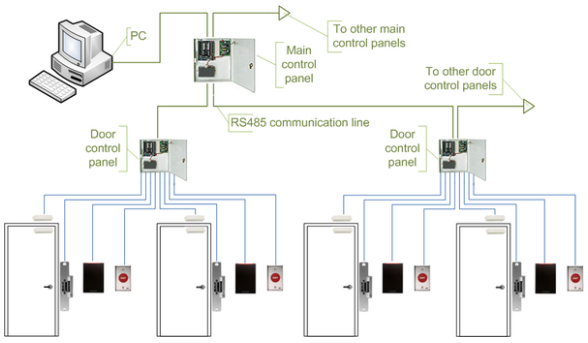
PC via a serial RS-485 communication line (or via 20mA current loop in some older systems). External RS-232/485 converters or internal RS-485 cards have to be installed, as standard PCs do not have RS-485 communication ports.

Advantages:

- RS-485 standard allows long cable runs, up to 4000 feet (1200 m)
- Relatively short response time. The maximum number of devices on an RS-485 line is limited to 32, which means that the host can frequently request status updates from each device, and display events almost in real time.
- High reliability and security as the communication line is not shared with any other systems.

Disadvantages:

- RS-485 does not allow Star-type wiring unless splitters are used
- RS-485 is not well suited for transferring large amounts of data (i.e. configuration and users). The highest possible throughput is 115.2 kbit/sec, but in most system it is downgraded to 56.2 kbit/sec, or less, to increase reliability.
- RS-485 does not allow the host PC to communicate with several controllers connected to the same port simultaneously. Therefore in large systems, transfers of configuration, and users to controllers may take a very long time, interfering with normal operations.
- Controllers cannot initiate communication in case of an alarm. The host PC acts as a master on the RS-485 communication line, and controllers have to wait until they are polled.
- Special serial switches are required, in order to build a redundant host PC setup.
- Separate RS-485 lines have to be installed, instead of using an already existing network infrastructure.
- Cable that meets RS-485 standards is significantly more expensive than regular Category 5 UTP network cable.
- Operation of the system is highly dependent on the host PC. In the case that the host PC fails, events from controllers are not retrieved, and functions that require interaction between controllers (i.e. anti-passback) stop working.



Access control system using serial main and sub-controllers

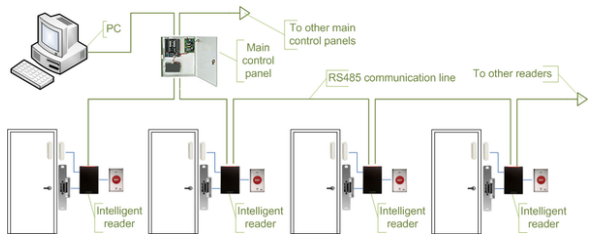
2. Serial main and sub-controllers. All door hardware is connected to sub-controllers (a.k.a. door controllers or door interfaces). Sub-controllers usually do not make access decisions, and instead forward all requests to the main controllers. Main controllers usually support from 16 to 32 sub-controllers.

Advantages:

- Work load on the host PC is significantly reduced, because it only needs to communicate with a few main controllers.
- The overall cost of the system is lower, as sub-controllers are usually simple and inexpensive devices.
- All other advantages listed in the first paragraph apply.

Disadvantages:

- Operation of the system is highly dependent on main controllers. In case one of the main controllers fails, events from its sub-controllers are not retrieved, and functions that require interaction between sub-controllers (i.e. anti-passback) stop working.
- Some models of sub-controllers (usually lower cost) have not the memory or processing power to make access decisions independently. If the main controller fails, sub-controllers change to degraded mode in which doors are either completely locked or unlocked, and no events are recorded. Such sub-controllers should be avoided, or used only in areas that do not require high security.
- Main controllers tend to be expensive, therefore such a topology is not very well suited for systems with multiple remote locations that have only a few doors.
- All other RS-485-related disadvantages listed in the first paragraph apply.



Access control system using serial main controller and intelligent readers

3. Serial main controllers & intelligent readers. All door hardware is connected directly to intelligent or semi-intelligent readers. Readers usually do not make access decisions, and forward all requests to the main controller. Only if the connection to the main controller is unavailable, will the readers use their internal database to make access decisions and record events. Semi-intelligent reader that have no database and cannot function without the main controller should be used only in areas that do not require high security. Main controllers usually support from 16 to 64 readers. All advantages and disadvantages are the same as the ones listed in the second paragraph.

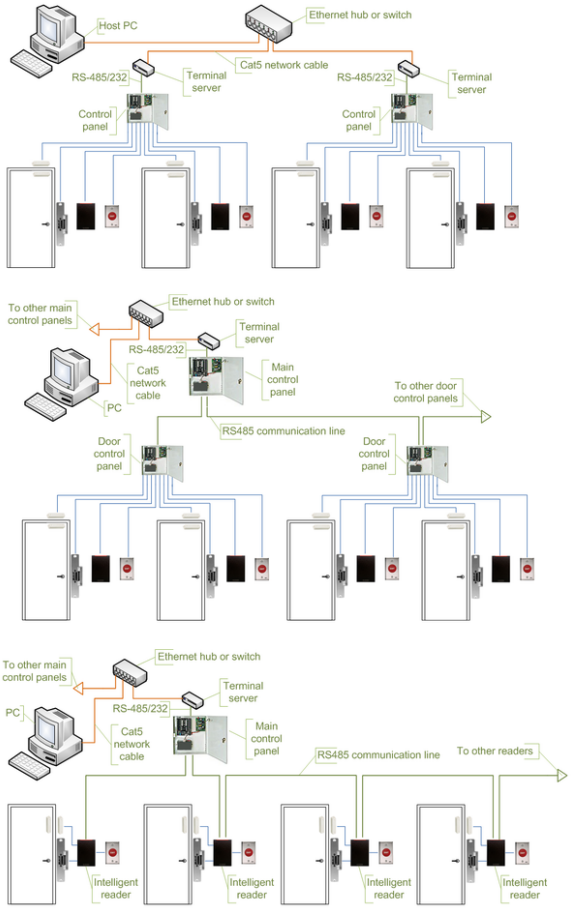
4. Serial controllers with terminal servers. In spite of the rapid development and increasing use of computer networks, access control manufacturers remained conservative, and did not rush to introduce network-enabled products. When pressed for solutions with network connectivity, many chose the option requiring less efforts: addition of a terminal server, a device that converts serial data for transmission via LAN or WAN.

Advantages:

- Allows utilizing the existing network infrastructure for connecting separate segments of the system.
- Provides a convenient solution in cases when the installation of an RS-485 line would be difficult or impossible.

Disadvantages:

- Increases complexity of the system.
- Creates additional work for installers: usually terminal servers have to be configured independently, and not through the interface of the access control software.
- Serial communication link between the controller and the terminal server acts as a bottleneck: even though the data between the host PC and the terminal server travels at the 10/100/1000Mbit/sec network speed, it must slow down to the serial speed of 112.5 kbit/sec or less. There are also additional delays introduced in the process of conversion between serial and network data.

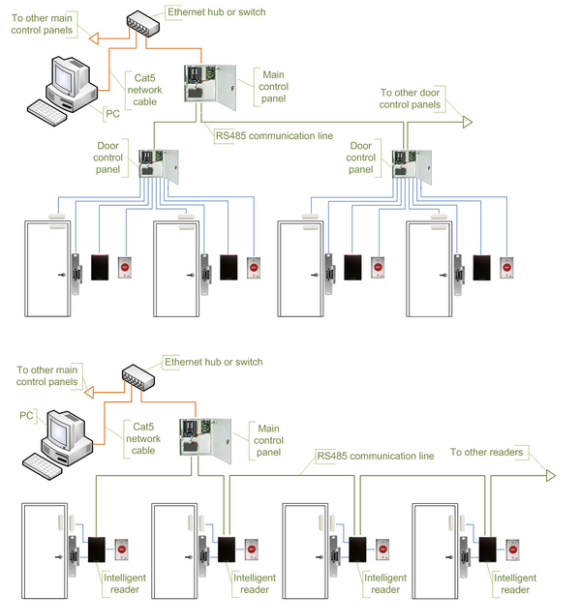


Access control systems using serial controllers and terminal servers

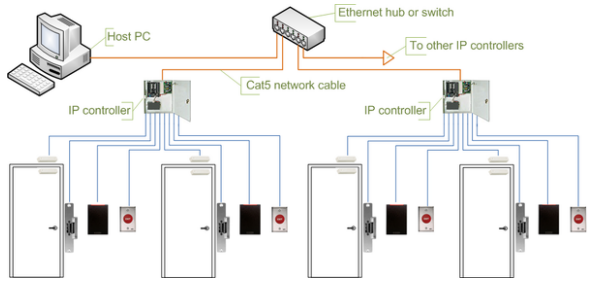
All the RS-485-related advantages and disadvantages also apply.

5. Network-enabled main controllers. The topology is nearly the same as described in the second and third paragraphs. The same advantages and disadvantages apply, but the on-board network interface offers a couple of valuable improvements. Transmission of configuration and user data to the main controllers is faster, and may be done in parallel. This makes the system more responsive, and does not interrupt normal operations. No special hardware is required in order to achieve redundant host PC setup: in the case that the primary host PC fails, the secondary host PC may start polling network controllers. The disadvantages introduced by terminal servers (listed in the fourth paragraph) are also eliminated.

6. IP controllers. Controllers are connected to a host PC via Ethernet LAN or WAN.



Access control system using network-enabled main controllers



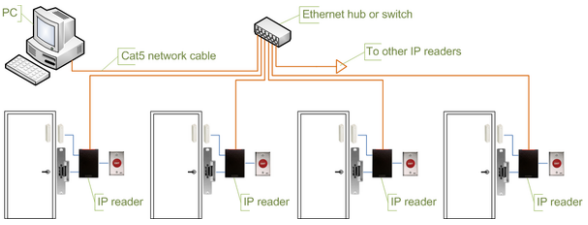
Access control system using IP controllers

Advantages:

- An existing network infrastructure is fully utilized, and there is no need to install new communication lines.
- There are no limitations regarding the number of controllers (as the 32 per line in cases of RS-485).
- Special RS-485 installation, termination, grounding and troubleshooting knowledge is not required.
- Communication with the controllers may be done at the full network speed, which is important if transferring a lot of data (databases with thousands of users, possibly including biometric records).
- In case of an alarm, controllers may initiate connection to the host PC. This ability is important in large systems, because it serves to reduce network traffic caused by unnecessary polling.
- Simplifies installation of systems consisting of multiple sites that are separated by large distances. A basic Internet link is sufficient to establish connections to the remote locations.
- Wide selection of standard network equipment is available to provide connectivity in various situations (fiber, wireless, VPN, dual path, PoE)

Disadvantages:

- The system becomes susceptible to network related problems, such as delays in case of heavy traffic and network equipment failures.
- Access controllers and workstations may become accessible to hackers if the network of the organization is not well protected. This threat may be eliminated by physically separating the access control network from the network of the organization. Also it should be noted that most IP controllers utilize either Linux platform or proprietary operating systems, which makes them more difficult to hack. Industry standard data encryption is also used.
- Maximum distance from a hub or a switch to the controller (if using a copper cable) is 100 meters (330 ft).
- Operation of the system is dependent on the host PC. In case the host PC fails, events from controllers are not retrieved and functions that require interaction between controllers (i.e. anti-passback) stop working. Some controllers, however, have a peer-to-peer communication option in order to reduce dependency on the host PC.



Access control system using IP readers

7. IP readers. Readers are connected to a host PC via Ethernet LAN or WAN.

Advantages:

- Most IP readers are PoE capable. This feature makes it very easy to provide battery backed power to the entire system, including the locks and various types of detectors (if used).

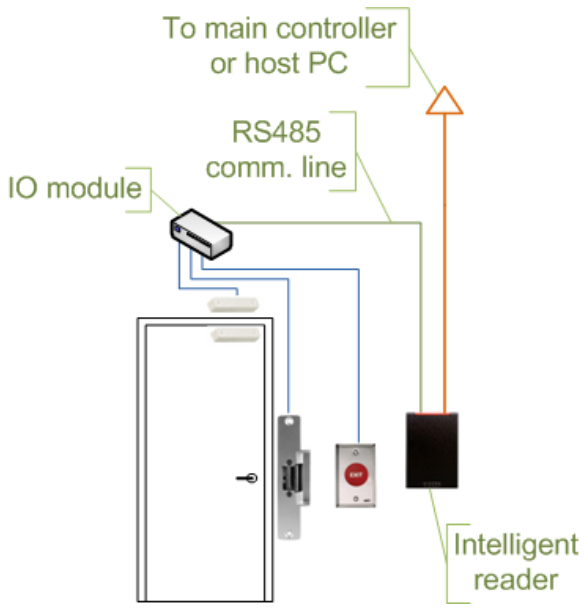
- IP readers eliminate the need for controller enclosures.
- There is no wasted capacity when using IP readers (e.g. a 4-door controller would have 25% of unused capacity if it was controlling only 3 doors).
- IP reader systems scale easily: there is no need to install new main or sub-controllers.
- Failure of one IP reader does not affect any other readers in the system.

Disadvantages:

- In order to be used in high-security areas, IP readers require special input/output modules to eliminate the possibility of intrusion by accessing lock and/or exit button wiring. Not all IP reader manufacturers have such modules available.
- Being more sophisticated than basic readers, IP readers are also more expensive and sensitive, therefore they should not be installed outdoors in areas with harsh weather conditions, or high probability of vandalism, unless specifically designed for exterior installation. A few manufacturers make such models.

The advantages and disadvantages of IP controllers apply to the IP readers as well.

7.1.7 Security risks



Access control door wiring when using intelligent readers and IO module

The most common security risk of intrusion through an access control system is by simply following a legitimate user through a door, and this is referred to as "tailgating". Often the legitimate user will hold the door for the intruder. This risk can be minimized through security awareness training of the user population, or more active means such as turnstiles. In very high security applications this risk is minimized by using a sally port, sometimes called a security vestibule or mantrap, where operator intervention is required presumably to assure valid identification.

The second most common risk is from levering a door open. This is surprisingly simple and effective on most doors. The lever could be as small as a screwdriver or big as a crow bar. Fully implemented access control systems include forced door monitoring alarms. These vary in effectiveness, usually failing from high false positive alarms, poor database configuration, or lack of active intrusion monitoring.

Similar to levering is crashing through cheap partition walls. In shared tenant spaces the divisional wall is a vulnerability. A vulnerability along the same lines is the breaking of sidelights.

Spoofing locking hardware is fairly simple and more elegant than levering. A strong magnet can operate the solenoid controlling bolts in electric locking hardware. Motor locks, more prevalent in Europe than in the US, are also susceptible to this attack using a doughnut shaped magnet. It is also possible to manipulate the power to the lock either by removing or adding current.

Access cards themselves have proven vulnerable to sophisticated attacks. Enterprising hackers have built portable readers that capture the card number from a user's proximity card. The hacker simply walks by the user, reads the card, and then presents the number to a reader securing the door. This is possible because card numbers are sent in the clear, no encryption being used.

Finally, most electric locking hardware still have mechanical keys as a fail-over. Mechanical key locks are vulnerable to bumping.

The need-to-know principle

The need to know principle can be enforced with user access controls and authorization procedures and its objective is to ensure that only authorized individuals gain access to information or systems necessary to undertake their duties. See Principle of least privilege.

7.2 Computer security

Further information: Computer access control

In computer security, general access control includes authorization, authentication, access approval, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

In any access-control model, the entities that can perform actions on the system are called *subjects*, and the entities representing resources to which access may need to be controlled are called *objects* (see also Access Control Matrix). Subjects and objects should both be considered as software entities, rather than as human users: any human users can only have an effect on the system via the software entities that they control.

Although some systems equate subjects with *user IDs*, so that all processes started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the principle of least privilege, and arguably is responsible for the prevalence of malware in such systems (see computer insecurity).

In some models, for example the object-capability model, any software entity can potentially act as both subject and object.

As of 2014, access-control models tend to fall into one of two classes: those based on capabilities and those based on access control lists (ACLs).

- In a capability-based model, holding an unforgettable reference or *capability* to an object provides access to the object (roughly analogous to how possession of one's house key grants one access to one's house); access is conveyed to another party by transmitting such a capability over a secure channel
- In an ACL-based model, a subject's access to an object depends on whether its identity appears on a list associated with the object (roughly analogous to how a bouncer at a private party would check an ID to see if a name appears on the guest list); access is conveyed by editing the list. (Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited.)

Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a *group* of subjects (often the group is itself modeled as a subject).

Access control systems provide the essential services of *authorization*, *identification and authentication* (*I&A*), *access approval*, and *accountability* where:

- authorization specifies what a subject can do
- identification and authentication ensure that only legitimate subjects can log on to a system
- access approval grants access during operations, by association of users with the resources that they are allowed to access, based on the authorization policy
- accountability identifies what a subject (or all subjects associated with a user) did

7.3 Access Control

Access to accounts can be enforced through many types of controls.*[9]

1. Mandatory Access Control (MAC)
   In MAC, users do not have much freedom to determine who has access to their files. For example, security clearance of users and classification of data (as confidential, secret or top secret) are used as security labels to define the level of trust.
2. Discretionary Access Control (DAC)
   In DAC, the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.
3. Role-Based Access Control (RBAC)
   RBAC allows access based on the job title. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.
4. Rule-Based Access Control
   An example of this would be only allowing students to use the labs during a certain time of the day.
5. Organization-Based Access control (OrBAC)
   OrBAC model allows the policy designer to define a security policy independently of the implementation*[10]

6. Responsibility Based Access control
   Information is accessed based on the responsibilities assigned to an actor or a business role*[11]

7.4 Telecommunication

In telecommunication, the term *access control* is defined in U.S. Federal Standard 1037C*[12] with the following meanings:

1. A service feature or technique used to permit or deny use of the components of a communication system.
2. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.
3. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device.
4. The process of limiting access to the resources of an AIS (Automated Information System) to authorized users, programs, processes, or other systems.
5. That function performed by the resource controller that allocates system resources to satisfy user requests.

This definition depends on several other technical terms from Federal Standard 1037C.

7.5 Public policy

In public policy, access control to restrict access to systems ("authorization") or to track or monitor behavior within systems ("accountability") is an implementation feature of using trusted systems for security or social control.

7.6 See also

- Security, Security engineering, Security lighting, Security Management, Security policy
- Alarm devices, Alarm management, Burglar alarm
- Door security, Lock picking, Lock smithing, Electronic lock, Safe, Safe-cracking, Bank vault
- Card reader, Common Access Card, Magnetic stripe card, Proximity card, Smart card, Swipe card, Optical turnstile, Access badge
- Identity management, ID Card, OpenID, IP Controller, IP reader
- Key management, Key cards
- Computer security, Logical security, Htaccess, Wiegand effect, XACML, Credential, Dual Unit
- Fingerprint scanner, Photo identification, Biometrics
- Physical Security Information Management - PSIM
- Physical Security Professional
- Prison, Razor wire, Mantrap
- Castle, Fortification

7.7 References

[1] RFC 4949

[2] Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment". Retrieved 2009-12-31.

[3] "MicroStrategy's office of the future includes mobile identity and cybersecurity". Washington Post. 2014-04-14. Retrieved 2014-03-30.

[4] biometric access control technology overview

[5] "iPhone 5S: A Biometrics Turning Point?". BankInfoSecurity.com. 2013-09-16. Retrieved 2014-03-30.

[6] "NFC access control: cool and coming, but not close". Security Systems News. 2013-09-25. Retrieved 2014-03-30.

[7] "Ditch Those Tacky Key Chains: Easy Access with EC Key". Wireless Design and Development. 2012-06-11. Retrieved 2014-03-31.

[8] isonas.com

[9] http://www.evolllution.com/media_resources/cybersecurity-access-control/

[10] http://orbac.org

[11] http://ceur-ws.org/Vol-599/BUISTAL2010_Paper5.pdf

[12] http://www.its.bldrdoc.gov/fs-1037/other/a.pdf

- U.S. Federal Standard 1037C
- U.S. MIL-STD-188
- U.S. National Information Systems Security Glossary

- Harris, Shon, All-in-one CISSP Exam Guide, 6th Edition, McGraw Hill Osborne, Emeryville, California, 2012.
- "Integrated Security Systems Design" - Butterworth/Heinenmann - 2007 - Thomas L. Norman, CPP/PSP/CSC Author
- Government Open Source Access Control —Next Generation (GOSAC-N)
- NIST.gov - Computer Security Division - Computer Security Resource Center - ATTRIBUTE BASED ACCESS CONTROL (ABAC) - OVERVIEW

7.8 External links

- eXtensible Access Control Markup Language. An OASIS standard language/model for access control. Also XACML.
- Access Control Systems

Chapter 8

Alarm device

"Alarm" redirects here. For other uses, see Alarm (disambiguation).

An **alarm device** or system of alarm devices gives an audible, visual or other form of alarm signal about a problem or condition. Alarm devices are often outfitted with a siren.

Alarm devices include:

- burglar alarms, designed to warn of burglaries; this is often a silent alarm: the police or guards are warned without indication to the burglar, which increases the chances of catching him or her.
- alarm clocks can produce an alarm at a given time
- distributed control systems (DCS), found in nuclear power plants, refineries and chemical facilities also generate alarms to direct the operator's attention to an important event that he or she needs to address.
- alarms in an operation and maintenance (O&M) monitoring system, which informs the bad working state of (a particular part of) the system under monitoring.
  - first-out alarm
- safety alarms, which go off if a dangerous condition occurs. Common public safety alarms include:
  - civil defense siren also known as *tornado sirens* or *air raid sirens*
  - fire alarm systems
    - fire alarm notification appliance
    - "Multiple-alarm fire", a locally-specific measure of the severity of a fire and the fire-department reaction required.
    - smoke detector
  - car alarms
  - autodialer alarm, also known as *community alarm*
  - personal alarm
  - tocsins – a historical method of raising an alarm

Alarms have the capability of causing a fight-or-flight response in humans; a person under this mindset will panic and either flee the perceived danger or attempt to eliminate it, often ignoring rational thought in either case. We can characterise a person in such a state as "alarmed".

With any kind of alarm, the need exists to balance between on the one hand the danger of false alarms (called "false positives") —the signal going off in the absence of a problem —and on the other hand failing to signal an actual problem (called a "false negative"). False alarms can waste resources expensively and can even be dangerous. For example, false alarms of a fire can waste firefighter manpower, making them unavailable for a real fire, and risk injury to firefighters and others as the fire engines race to the alleged fire's location. In addition, false alarms may acclimatise people to ignore alarm signals, and thus possibly to ignore an actual emergency: Aesop's fable of *The Boy Who Cried Wolf* exemplifies this problem.

8.1 Etymology

The word came from the Old French *À l'arme* meaning "To the arms", "To the weapons", telling armed men to pick up their weapons and get ready for action, because an enemy may have suddenly appeared.

8.2 See also

- Alarm management
- Warning system
- False alarm
- Physical security

Chapter 9

Motion detection

Motion detection is the process of detecting a change in position of an object relative to its surroundings or the change in the surroundings relative to an object. Motion detection can be achieved by both mechanical and electronic methods. When motion detection is accomplished by natural organisms, it is called motion perception.

Motion can be detected by:

1. Infrared (Passive and active sensors)
2. Optics (video and camera systems)
3. Radio Frequency Energy (radar, microwave and tomographic motion detection)
4. Sound (microphones and acoustic sensors)
5. Vibration (triboelectric, seismic, and inertia-switch sensors)
6. Magnetism (magnetic sensors and magnetometers)

Motion detecting devices include:

1. Sony Computer Entertainment's PlayStation Move or PlayStation Eye for PS3 and PlayStation Camera for PS4
2. Microsoft Corporation's Kinect for Xbox 360, Windows 7, 8, 8.1 or Xbox One
3. Nintendo's Wii Remote
4. ASUS Eee Stick
5. HP's Swing

9.1 Mechanical

The most basic form of mechanical motion detection is in the form of a switch or trigger. These motion detection devices are common in our everyday lives. The keys of a typewriter, or even the keys on the keyboards used to type this article employ a mechanical method of detecting motion. Each key is a manual switch that is either off or on. Each letter that appears is a result of motion on that corresponding key and the switch being turned on. This simple binary code concept is at the heart of the digital age, with mechanical switches being replaced by ever shrinking transistors.*[1]*[2]

9.2 Electronic

See also: Motion estimation

The principal methods by which motion can be electronically identified are optical detection and acoustical detection. Infrared light or laser technology may be used for optical detection. Motion detection devices, such as PIR motion detectors, have a sensor that detects a disturbance in the infrared spectrum, such as a person or an animal. Once detected, an electronic signal can activate an alarm or a camera that can capture an image or video of the motioner.*[3]*[4]

The chief applications for such detection are (a) detection of unauthorized entry, (b) detection of cessation of occupancy of an area to extinguish lighting and (c) detection of a moving object which triggers a camera to record subsequent events. The motion detector is thus a linchpin of electronic security systems, but is also a valuable tool in preventing the illumination of unoccupied spaces.*[5]

A simple algorithm for motion detection by a fixed camera compares the current image with a reference image and simply counts the number of different pixels. Since images will naturally differ due to factors such as varying lighting, camera flicker, and CCD dark currents, pre-processing is useful to reduce the number of false positive alarms.

More complex algorithms are necessary to detect motion when the camera itself is moving, or when the motion of a specific object must be detected in a field containing other

movement which can be ignored. An example might be a painting surrounded by visitors in an art gallery.

9.3 Occupancy sensors for lighting control

Motion sensors are often used in indoor spaces to control electric lighting. If no motion is detected, it is assumed that the space is empty, and thus does not need to be lit. Turning off the lights in such circumstances can save substantial amounts of energy. In lighting practice occupancy sensors are sometime also called "presence sensors" or "vacancy sensors". Some occupancy sensors (e.g. LSG's Pixelview, Philips Lumimotion, Ecoamicatechs Sirius etc.) also classify the number of occupants, their direction of motion, etc., through image processing. Pixelview is a camera-based occupancy sensor, using a camera that is built into each light fixture.

9.3.1 System design and components

Occupancy sensors for lighting control typically use infrared (IR), ultrasonic, tomographic motion detection, microwave sensors, or camera-based sensors (image processing).*[6] The field of view of the sensor must be carefully selected/adjusted so that it responds only to motion in the space served by the controlled lighting. For example, an occupancy sensor controlling lights in an office should not detect motion in the corridor outside the office. Tomographic motion detection systems have the unique benefit of detecting motion through walls and obstructions, yet do not trigger as easily from motion on the outside of the detection area like traditional microwave sensors.

Sensors and their placement are never perfect, therefore most systems incorporate a delay time before switching. This delay time is often user-selectable, but a typical default value is 15 minutes. This means that the sensor must detect no motion for the entire delay time before the lights are switched. Most systems switch lights off at the end of the delay time, but more sophisticated systems with dimming technology reduce lighting slowly to a minimum level (or zero) over several minutes, to minimize the potential disruption in adjacent spaces. If lights are off and an occupant re-enters a space, most current systems switch lights back on when motion is detected. However, systems designed to switch lights off automatically with no occupancy, and that require the occupant to switch lights on when they re-enter are gaining in popularity due to their potential for increased energy savings. These savings accrue because in a spaces with access to daylight the occupant may decide on their return that they no longer require supplemental electric light.*[7]

9.4 See also

- Motion detector
- Motion controller for video game consoles

9.5 References

[1] Switching Circuits and Boolean Algebra

[2] Talking Electronics, Transistors

[3] Video motion detection (VMD)

[4] Mechanisms of visual motion

[5] HowStuffWorks.com "Motion Detection"

[6] "Technology comparison of Occupancy sensors". Retrieved 19 July 2014.

[7] Did It Move? Detecting Motion with PIR + Arduino

9.6 External links

- Relational Motion Detection
- www.cs.rochester.edu/~{ }nelson/research
- Motion Detection Algorithms In Image Processing
- Motion Detection and Recognition Research
- Presence and Absence detection explained
- Motion detection sample algorithm realization video

Chapter 10

Glass break detector

Passive glass break detector

A **glass break detector** is a sensor used in electronic burglar alarms that detects if a pane of glass is shattered or broken. These sensors are commonly used near glass doors or glass store-front windows to detect if an intruder broke the glass and entered.

Glass break detectors usually use a microphone, which monitors any noise or vibrations coming from the glass. If the vibrations exceed a certain threshold (that is sometimes user selectable) they are analyzed by detector circuitry. Simpler detectors simply use narrowband microphones tuned to frequencies typical of glass shattering, and react to sound above certain threshold, whereas more complex designs compare the sound analysis to one or more glass-break profiles using signal transforms similar to DCT and FFT and react if both the amplitude threshold and statistically expressed similarity threshold are breached.

10.1 See also

- Chubb Locks
- Yale (company)
- Burglar alarm

10.2 External links

Chapter 11

Identity document

"National identity card" redirects here. For cards referred to in the English language as "national identity card", see National identity card (disambiguation).

An **identity document** (also called a **piece of identification** or **ID**, or colloquially as one's 'papers') is any document which may be used to verify aspects of a person's personal identity. If issued in the form of a small, mostly standard-sized card, it is usually called an **identity card** (**IC** or **ID card**). Countries which do not have formal identity documents may require identity verification using informal documents.

In the absence of a formal identity document, driving licences may be accepted in many countries for identity verification. Some countries do not accept driving licences for identification, often because in those countries they do not expire as documents and can be old or easily forged. Most countries accept passports as a form of identification.

Some countries require foreigners to have a passport or occasionally a national identity card from their country available at any time if they do not have residence permit in the country.

The personal information present on the identity document, or in a supporting database, might include the bearer's full name, a portrait photo, age, birth date, address, an identification number, profession or rank, religion, ethnic or racial classification, restrictions, and citizenship status.

11.1 History

The version of the passport introduced by King Henry V of England in the Safe Conducts Act 1414 is considered to be the earliest identity document inscribed into law.*[1]

Before World War I, most people did not have or need an identity document.

Photographs began to be attached to passports and other "photo IDs" in the early 20th century, after photography technology became widespread.

The shape and size of identity cards were standardized in 1985 by ISO/IEC 7810. Some modern identity documents are smart cards including a difficult-to-forge embedded integrated circuit, that were standardized in 1988 by ISO/IEC 7816. New technologies allows identity cards to contain biometric information, such as photographs, face, hand or iris measurements, or fingerprints. Electronic identity cards (or e-IDs) are already available in countries including Hong Kong, Malaysia, Estonia, Finland, Belgium, Guatemala, Portugal, Morocco and Spain.

11.2 Adoption of identity cards

The universal adoption of identity cards is supported by law enforcement officials who claim that it makes surveillance and identification of criminals easier. However, concern is also expressed about the extensive cost and potential abuse of high-tech smartcards.

In the United Kingdom and the United States especially, government-issued compulsory identity cards or, more precisely, their centralised database are a source of debate as they are regarded as an infringement of privacy and civil liberties. Most criticism is directed towards the enhanced possibilities of extensive abuse of centralised and comprehensive databases storing sensitive data. A 2006 survey of UK Open University students concluded that the planned compulsory identity card under the Identity Cards Act 2006 coupled with a central government database generated the most negative attitudinal response among several alternative configurations.

11.2.1 Arguments for

- In order to avoid mismatching people, and to fight fraud, there should be a way, as securely as possible, to prove a person's identity.

- Every human being already carries one's own personal identification in the form of one's DNA, which cannot be falsified or discarded. Even for non-state commercial and private interactions, this may shortly become the preferred identifier, rendering a state-issued identity card a lesser evil than the potentially extensive privacy risks associated with everyday use of a person's genetic profile for identification purposes.*[2]*[3]*[4]*[5]*[6]

11.2.2 Arguments against

Further information: freedom of movement and Propiska

Arguments against identity documents as such:

- The development and administration costs of an identity card system can be very high. Figures from £30 (US$45) to £90 or even higher have been suggested for the proposed UK ID card. In countries like Chile the identity card is personally paid for by each person up to £6; in other countries, such as Venezuela, the ID card is free.*[7] This, however, does not disclose true cost of issuing ID cards as some additional portion may be borne by taxpayers in general.

Arguments against national identity documents:

- Rather than relying on government-issued ID cards, federal policy has the alternative to encourage the variety of identification systems that exist in the private marketplace today. These private systems can provide better assurance of identity and trustworthiness than many government-issued ID cards.*[8] However, the inherent lack of consistency regarding issuance policies can lead to downstream problems. For example, in Sweden private companies such as banks (citing security reasons) refused to issue ID cards to individuals without a Swedish card. This forced the government to start issuing national cards.

Arguments against overuse or abuse of identity documents:

- Cards reliant on a centralized database can be used to track anyone's physical movements and private life, thus infringing on personal freedom and privacy. The proposed British ID card (see next section) proposes a series of linked databases managed by private sector firms. The management of disparate linked systems across a range of institutions and any number of personnel is alleged to be a security disaster in the making.*[9]
- If religion or ethnicity is registered on mandatory ID documents, this data can enable racial profiling.

11.3 National policies

Main article: List of identity card policies by country

According to Privacy International, as of 1996, possession of identity cards was compulsory in about 100 countries, though what constitutes "compulsory" varies. In some countries (see below), it is compulsory to have an identity card when a person reaches a prescribed age. The penalty for non-possession is usually a fine, but in some cases it may result in detention until identity is established. For people suspected with crimes such as shoplifting or no bus ticket, non-possession might result in such detention, also in countries not formally requiring identity cards. In practice, random checks are rare, except in certain times.

A number of countries do not have national identity cards. These include Australia, Canada, Denmark, Ireland, India (see below), Japan, New Zealand, Norway, the United Kingdom and the United States. Other identity documents such as passport or drivers license is then used as identity documents when needed.

A number of countries have voluntary identity card schemes. These include Austria, Finland, France (see France section), Hungary (however, all citizens of Hungary must have at least one of: valid passport, photocard driving licence, or the National ID card), Iceland, Sweden and Switzerland. The United Kingdom's scheme was scrapped in January 2011 and the database was destroyed.

In the United States, states issue optional identity cards for people who do not hold a driver's license as an alternate means of identification. These cards are issued by the same organization responsible for driver's licenses, usually called the Department of Motor Vehicles.

For the Sahrawi people of Western Sahara, pre-1975 Spanish identity cards are the main proof that they were Saharaui citizens as opposed to recent Moroccan colonists. They would thus be allowed to vote in an eventual self-determination referendum.

Companies and government departments may issue ID cards for security purposes or proof of a qualification. For example, all taxicab drivers in the UK carry ID cards. Managers, supervisors, and operatives in construction in the UK have a photographic ID card, the CSCS (Construction Skills Certification Scheme) card, indicating training and skills including safety training. Those working on UK railway lands near working lines must carry a photographic ID card to indicate training in track safety (PTS and other cards) posses-

sion of which is dependent on periodic and random alcohol and drug screening. In Queensland and Western Australia, anyone working with children has to take a background check and get issued a Blue Card or Working with Children Card, respectively.

11.3.1 Africa

Egypt

It is compulsory for all Egyptian citizens age 16 or older to possess ID card (Arabic: بطاقة تحقيق شخصية *Biṭāqat taḥqīq shakhṣiyya*, literally, "Personal Verification Card"). In daily colloquial speech, it is generally simply called "el-biṭāqa *("the card"). It is used for:*

- Opening or closing a bank account
- Registering at a school or university
- registering the number of a mobile or landline telephone
- Interacting with most government agencies, including:
  - Applying for or renewing a driver's license
  - Applying for a passport
  - Applying for any social services or grants
  - Registering to vote, and voting in elections
  - Registering as a taxpayer

Egyptian ID cards expire after 7 years from the date of issue. Some feel that Egyptian ID cards are problematic, due to the general poor quality of card holders' photographs and the compulsory requirements for ID card holders to identify their religion and for married women to use their husband's surname.

Tunisia

Every citizen of Tunisia is expected to apply for an ID card by the age of 18; however, with the approval of a parent, a Tunisian citizen may apply for, and receive, an ID card prior to their eighteenth birthday.

Gambia, The

All Gambian citizens over 18 years of age are required to hold a Gambian National Identity Card. In July 2009, a new biometric Identity card was introduced. The biometric National Identity card is one of the acceptable documents required to apply for a Gambian Driver License.

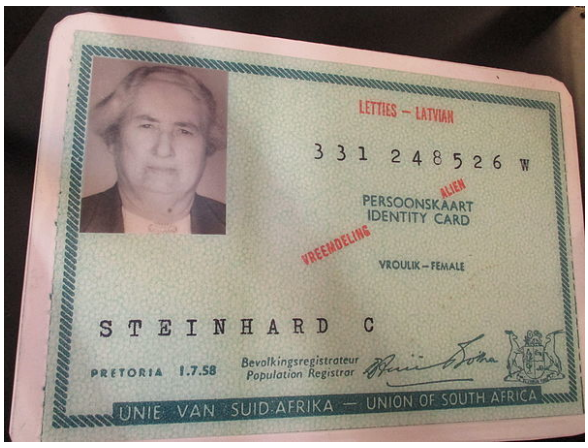
Mauritius

Mauritius requires all citizens who have reached the age of 18 to apply for a National Identity Card. The National Identity Card is one of the few accepted forms of identification, along with passports. A National Identity Card is needed to apply for a passport for all adults, and all minors must take with them the National Identity Card of a parent when applying for a passport.*[10]

Nigeria

Nigeria first introduced a National Identity Card in 2005, but its adoption back then was limited and not widespread. The country is now in the process of introducing a new biometric ID Card complete with a SmartCard and other security features. The National Identity Management Commission (NIMC) *[11] is the Federal Government Agency responsible for the issuance of these new cards, as well as the management of the new National Identity Database. The Federal Government of Nigeria announced in April 2013 *[12] that after the next General Election in 2015, all subsequent elections will require that voters will only be eligible to stand for office or vote provided the Citizen possesses a NIMC-issued Identity Card. The Central Bank of Nigeria is also looking into instructing banks to request for a National Identity Number (NIN) for any citizen maintaining an account with any of the banks operating in Nigeria. The proposed kick off date is yet to be determined.

South Africa



Old South African identity card issued to a permanent resident (PR).

South African citizens aged 15 years and 6 months or older are eligible for an ID book. The South African identity document resembles a passport; however, it is not valid as a

travel document or valid for use outside South Africa. Although carrying the document is not required in daily life, it is necessary to show the document or a certified copy as proof of identity when:

- Signing a contract, including
  - Opening or closing a bank account
  - Registering at a school or university
  - Buying a mobile phone and registering the number
- Interacting with most government agencies, including
  - Applying for or renewing a driver's license or firearm licence
  - Applying for a passport
  - Applying for any social services or grants
  - Registering to vote, and voting in elections
  - Registering as a taxpayer or for unemployment insurance

The South African "ID Book" used to also contain driving and firearm licences; however, these documents are now issued separately in card format. In mid 2013 a smart card ID was launched to replace the ID book. The cards were launched on 18 July 2013 when a number of dignitaries received the first cards at a ceremony in Pretoria.*[13] The government plans to have the ID books phased out over a six to eight-year period.*[14] The South African government is looking into possibly using this smart card not just as an identification card but also for licences, National Health Insurance, and social grants.*[15]

Zimbabwe

Zimbabweans are required to apply for National Registration at the age of sixteen. Zimbabwean citizens are issued with a plastic card which contains a photograph and their particulars onto it. Before the introduction of the plastic card, the Zimbabwean ID card used to be printed on anodised aluminium. Along with drivers licences, the National Registration Card (including the old metal type) is universally accepted as proof of identity in Zimbabwe. Zimbabweans are required by law to carry identification on them at all times and visitors to Zimbabwe are expected to carry their passport with them at all times.

11.3.2 Asia

Bahrain

Bahrain citizens have must have both an ID card called "smart card" that is recognized as an official document and can be used within the Gulf Cooperation Council and a passport that is recognized worldwide.

Bangladesh

Biometric identification has existed in Bangladesh since 2008. All Bangladeshis who are 18 years of age and older are included in a central Biometric Database, which is used by the Bangladesh Election Commission to oversee the electoral procedure in Bangladesh. All Bangladeshis are issued with an *NID Card* which can be used to obtain a passport, driving licence, credit card, and to register land ownership.

China

Main article: Resident Identity Card (PRC)

The People's Republic of China requires every citizen

Sample of the second generation ID card issued in China

above the age of 16 to carry an identity card. The card is the only acceptable legal document to obtain a resident permit, employment, open bank accounts, obtain a passport, driver's license, for application to tertiary education and technical colleges.

Hong Kong

Main article: Hong Kong Identity Card

The **Hong Kong Identity Card** (or **HKID**) is an official

Hong Kong Permanent ID card

identity document issued by the Immigration Department of Hong Kong to all people who hold the right of abode, right to land or other forms of limited stay longer than 180 days in Hong Kong. According to Basic Law of Hong Kong, all permanent residents are eligible to obtain the **Hong Kong Permanent Identity Card** which states that the holder has the right of abode in Hong Kong.

India

Main article: Unique Identification Authority of India

Multi-purpose national identity cards, carrying 16 personal details and a unique identification number are issued to all citizens since 2007. Biometric data such as fingerprints and a digital signature are contained in a microchip embedded in the card. On it are details of the holder's date and place of birth and a unique 16-digit National Identification Number. The card has a SCOSTA QR code embedded on the card, through which all the details on the card are accessible.*[16]

Indonesia

Main article: Indonesian identity card

Residents over 17 are required to hold a KTP (Kartu Tanda Penduduk) identity card. The card will identifies whether the holder is an Indonesian citizen or foreign national. In 2011, the Indonesian government started a two-year ID issuance campaign that utilizes smartcard technology and biometric duplication of fingerprint and iris recognition. This card, called the Electronic KTP (e-KTP), will replace the conventional ID (KTP) beginning in 2013. By 2013, it is estimated that approximately 172 million Indonesian nationals will have an e-KTP issued to them.

Iran

Every citizen of Iran has an Identification document called Shenasnameh(Persian:شناسنامه) which is a booklet based on their birth certificate, in the Shenasnameh National ID number, Birth date, Birthplace, Father and Mother names birth dates and National ID numbers would be registered. Also in other pages of the Shenasnameh Marriage status, Spouse(s) name(s), Children names, Date of every vote they give and also their death would be registered.*[17]

Every Iranian permanent resident above the age of 15 must hold a valid National Identity Card (Persian:کارت ملی) or at least obtain their unique National Number from any of the local Vital Records branches of the Iranian Ministry of Interior.*[18]

In order to apply for an NID card, the applicant must be at least 15 years old and have a photograph attached to their Birth Certificate, which is undertaken by the Vital Records branch.

Since June 21, 2008, NID cards have been compulsory for many things in Iran and Iranian Missions abroad (e.g. obtaining a passport, driver's license, any banking procedure,etc.)*[19]

Iraq

Every Iraqi citizen must have a personal/national card (البطاقة الشخصية) in Arabic.

Israel

Main article: Teudat Zehut

Israeli law requires every permanent resident above the age of 16, whether a citizen or not, to carry an identification card called *te'udat zehut* (Hebrew: תעודת זהות) in Hebrew or *biṭāqat huwīya* (بطاقة هوية) in Arabic.

The card is designed in a bilingual form, printed in Hebrew and Arabic, however, the personal data is presented in Hebrew by default and may be presented in Arabic as well if the owner decides so. The card must be presented to an official on duty (e.g. a policeman) upon request, but if the resident is unable to do this, one may contact the relevant authority within five days to avoid a penalty.

Until the mid-1990s, the identification card was considered the only legally reliable document for many actions such as voting or opening a bank account. Since then, the

new Israeli driver's licenses which include photos and extra personal information are now considered equally reliable for most of these transactions. In other situations any government-issued photo ID, such as a passport or a military ID, may suffice.

Palestinian Authority The Palestinian Authority Issues Identification card following agreements with Israel since 1995 in accordance to the Oslo Accords, the data is forwarded to Israeli database and confirmed. In February 2014, a presidential decision issued by Palestinian president Mahmoud Abbas to abolish the religion field was announced.*[20] Israel has objected to abolishing religion on Palestinian IDs because it controls their official records, IDs and passports and the PA does not have the right to make amendments to this effect without the prior approval of Israel, Palestinian Authority in Ramallah said that abolishing religion on the ID has been at the center of negotiations with Israel since 1995. The decision was criticized by Hamas officials in Gaza Strip, saying it is unconstitutional and will not be implemented in Gaza because it undermines the Palestinian cause.*[21]

Japan

Japanese citizens are not required to have identification documents with them within the territory of Japan. When necessary, official documents, such as one's Japanese driving license, basic resident registration card,*[22] radio operator license,*[23] social insurance card or passport are generally used and accepted. On the other hand, mid- to long term foreign residents are required to carry their Zairyū cards,*[24] while short term visitors and tourists (those with a Temporary Visitor status sticker in their passport) are required to carry their passports.

Macao

Main article: Macau Resident Identity Card

The Macao Resident Identity Card is an official identity document issued by the Identification Department to permanent residents and non-permanent residents.

Malaysia

Main article: MyKad

In Malaysia, the **MyKad** is the compulsory identity document for Malaysian citizens aged 12 and above. Introduced by the *National Registration Department of Malaysia* on 5 September 2001 as one of four MSC Malaysia flagship applications*[25] and a replacement for the **High Quality Identity Card** (*Kad Pengenalan Bermutu Tinggi*), Malaysia became the first country in the world to use an identification card that incorporates both photo identification and fingerprint biometric data on an in-built computer chip embedded in a piece of plastic.*[26]

Myanmar

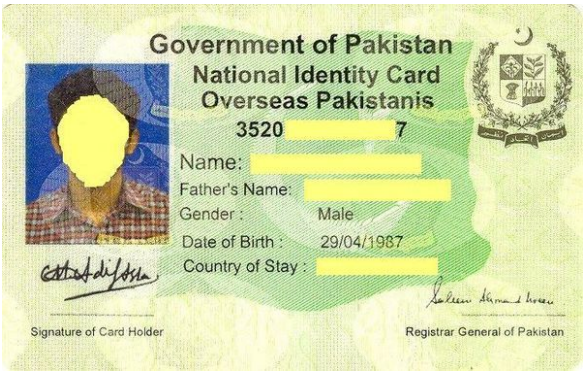
Main article: Burmese nationality law

Myanmar citizens are required to obtain a National Registration Card (NRC), while non-citizens are given a Foreign Registration Card (FRC).

Pakistan

Main article: Computerised National Identity Card

In Pakistan, all adult citizens must register for the Computerized National Identity Card (CNIC), with a unique number, at age 18. CNIC serves as an identification document to authenticate an individual's identity as the citizen of Pakistan.



Specimen Pakistan ID card

Earlier on, National Identity Cards (NICs) were issued to citizens of Pakistan. Now government has shifted all its existing records of National Identity Cards (NIC) to the central computerized database managed by NADRA. New CNIC's are machine readable and have security features such as facial and finger print information. By the end of 2013, all CNICs will be replaced by Smart national identity cards, SNICs.

Singapore

Main article: National Registration Identity Card

In Singapore, every citizen, and permanent resident (PR) must register at the age of 15 for an Identity Card (IC). The card is necessary not only for procedures of state but also in the day-to-day transactions of registering for a mobile phone line, obtaining certain discounts at stores, and logging on to certain websites on the internet. Schools frequently use it to identify students, both on-line and in exams.[*] [27]

Sri Lanka

Main article: National identity card (Sri Lanka)

In Sri Lanka, all citizens over the age of 16 need to apply for a National Identity Card (NIC). Each NIC has a unique 10 digit number, in the format 000000000A (where 0 is a digit and A is a letter). The first two digits of the number are your year of birth (e.g.: 93xxxxxxxx for someone born in 1993). The final letter is generally a 'V' or 'X'. An NIC number is required to apply for a passport (over 16), driving license (over 18) and to vote (over 18). In addition, all citizens are required to carry their NIC on them at all times as proof of identity, given the security situation in the country. NICs are not issued to non-citizens, who are still required to carry a form of photo identification (such as a photocopy of their passport or foreign driving license) at all times. At time the Postal ID card may also be used.

Taiwan

Main article: National Identification Card (Taiwan)

The "National Identification Card" (Chinese: 國民身分證) is issued to all nationals of the Republic of China (Official name of Taiwan) aged 14 and older who have household registration in the Taiwan Area. The Identification Card is used for virtually all other activities that require identity verification within Taiwan such as opening bank accounts, renting apartments, employment applications and voting.

Frontside of ID card issued in Taiwan

Backside of ID card issued in Taiwan

The Identification Card contains the holder's photo, ID number, Chinese name, and (Minguo calendar) date of birth. The back of the card also contains the person's registered address where official correspondence is sent, place of birth, and the names of parents and spouse.

If the person moves, one must re-register at a municipal office (Chinese: 戶政事務所).

ROC nationals with household registration in Taiwan are known as "registered nationals". ROC nationals who do not have household registration in Taiwan (known as "unregistered nationals") do not qualify for the Identification Card and its associated privileges (e.g. the right to vote and the right of abode in Taiwan), but qualify for the Republic of China passport, which unlike the Identification Card, is not indicative a residency rights in Taiwan. If such "unregistered nationals" are resident in Taiwan, they will hold a Taiwan Area Resident Certificate as an identity document, which is nearly identical to the Alien Resident Certificate issued to foreign nationals/citizens resident in Taiwan.

Thailand

Main article: Thai national ID card

In Thailand, The Thai National ID Card (Thai: บัตรประจำตัวประชาชน; RTGS: bat pracham tua pracha chon) is an official identity document, issued only to Thai Nationals. The purpose of the card is to prove and identify the holder's identity, for receiving government services and other entitlements.

United Arab Emirates

Emirates Identity Authority is responsible for the processing of residents and nationals for the mandatory identity card and population register in the United Arab Emirates.

Vietnam

In Vietnam, all citizens above 14 years old must possess a **People's Identity Card**.

People's Identity Card is provided by the local authority.

11.3.3 Europe

See also: National identity cards in the European Economic Area

European Union

See also: National identity cards in the European Union and PRADO - Public Register of Travel and Identity Documents Online

Within the European Union, identity cards meeting the official EU standard may also be used by a European citizen as a travel document in place of a passport.

During the UK Presidency of the EU in 2005 a decision was made to: "Agree common standards for security features and secure issuing procedures for ID cards (December 2005), with detailed standards agreed as soon as possible thereafter. In this respect, the UK Presidency has put forward a proposal for EU-wide use of biometrics in national identity cards." *[28]

Belgium Main article: Belgian national identity card

In Belgium, everyone above the age of 12 is issued an identity card (*carte d'identité* in French, *identiteitskaart* in Dutch and *Personalausweis* in German), and from the age of 15 carrying this card at all times is mandatory. For foreigners residing in Belgium similar cards (foreigner's cards, *vreemdelingenkaart* in Dutch, *carte pour étrangers* in French) are issued, although they may also carry a passport, a work permit or a (temporary) residence permit.

Since 2000, all newly issued Belgian identity cards have a chip (eID card), and roll-out of these cards is expected to be complete in the course of 2009. Since early 2009, the aforementioned foreigner's card has also been replaced by an eID card, containing a similar chip. The eID cards can be used both in the public and private sector for identification and for the creation of legally binding electronic signatures.

Belgian consulates still issue old style ID cards (105 x 75 mm) to Belgian citizens who are permanently residing in their jurisdiction and who choose to be registered at the consulate (which is strongly advised).

Bulgaria Main article: Bulgarian identity card

In Bulgaria, it is obligatory to possess an identity card (Bulgarian - лична карта, lichna karta) at the age of 14. Any person above 14 being checked by the police without carrying at least some form of identification is liable to a fine of 50 Bulgarian leva (about 25 Euros).

Bulgarian EU national biometric identity card

Croatian ID card specimen

Croatia Main article: Croatian identity card

All Croatian citizens may request an Identity Card. All persons over the age of 16 must have an Identity Card and carry it at all times. Refusal to carry or produce an Identity Card to a police officer can lead to a fine of 100 kuna or more

and detention until the individual's identity can be verified by fingerprints.

Croatian ID card is valid in the entire European Union, and can also be used to travel throughout the non-EU countries of the Balkans.

The 2013 design of the Croatian ID card is prepared for future installation of an Electronic identity card chip, which is set for implementation in 2014.*[29]

Cyprus The acquisition and possession of Civil Identity Card is compulsory for any eligible person who has completed twelve years of age.

Czech Republic Main article: Czech national identity card

An identity card with a photo is issued to all citizens of the Czech Republic at the age of 15. It is officially recognised by all member states of the European Union for intra EU travel. Travelling outside the EU mostly requires the Czech passport.

Denmark Denmark is one of few EU countries that currently do not issue national identity cards (not counting driving licences and passports issued for other purposes).

Danish citizens are not required by law to carry an identity card. A traditional identity document (without photo), the *personal identification number certificate* (Danish:*Personnummerbevis*) is of little use in Danish society, as it has been largely replaced by the much more versatile *National Health Insurance Card* (Danish:*Sundhedskortet*) which contains the same information and more. The National Health Insurance Card is issued to all citizens age 12 and above. It is commonly referred to as an identity card despite the fact it has no photo of the holder. Both certificates retrieve their information from the Civil Registration System. However, the *personnummerbevis* is still issued today and has been since September 1968.

Danish driver's licenses and passports are the only identity cards issued by the government containing both the personal identification number and a photo. A foreign citizen without driving skills living in Denmark can not get such documents. Foreign driver's licenses and passports are accepted with limitations. A foreigner living in Denmark will have a residence permit with their personal identification number and a photo.

In Denmark, counties issue since 2004 "photo identity card" (Danish: *billedlegitimationskort*), which can be used as age verification, but only limited for identification because of limited security for issuing, and not for EU travel. Until 2004, the national debit card Dankort contained a photo of the holder and was widely accepted as an identity card. The Danish banks lobbied successfully to have pictures removed from the national debit cards and so since 2004 the Dankort no longer contains a photo. Hence it is rarely accepted for identification.

Estonia Main article: Estonian ID card

The Estonian identity card (Estonian: *ID-kaart*) is a chipped picture ID in the Republic of Estonia. An Estonian identity card is officially recognised by all member states of the European Union for intra EU travel. For travelling outside the EU, Estonian citizens may also require a passport.

The card's chip stores a key pair, allowing users to cryptographically sign digital documents based on principles of public key cryptography using DigiDoc. Under Estonian law, since 15 December 2000 the cryptographic signature is legally equivalent to a manual signature.

The Estonian identity card is also used for authentication in Estonia's ambitious Internet-based voting programme. In February 2007, Estonia was the first country in the world to institute electronic voting for parliamentary elections. Over 30 000 voters participated in the country's first e-election.*[30] By 2014, at the European Parliament elections, the number of e-voters has increased to more than 100,000 comprising 31% of the total votes cast.*[31]

Finland Main article: Finnish identity card

In Finland, any citizen can get an identification card (*henkilökortti*/*identitetskort*). This, along with the passport, is one of two official identity documents. It is available as an electronic ID card (*sähköinen henkilökortti*/*elektroniskt identitetskort*), which enables logging into certain government services on the Internet.

Driving licenses and KELA (social security) cards with a photo are also widely used for general identification purposes even though they are not officially recognized as such. However, KELA has ended the practice of issuing social security cards with the photograph of the bearer, while it has become possible to embed the social security information onto the national ID card. For most purposes when identification is required, only valid documents are ID card, passport or driving license. However, a citizen is not required to carry any of these.

France Main article: French national identity card

France has had a national ID card for all citizens since the

beginning of World War II in 1940. Compulsory identity documents were created before, for workers from 1803 to 1890, nomads in 1912, and foreigners in 1917 during World War I. National identity cards were first issued as the *carte d'identité Française* under the law of October 27, 1940, and were compulsory for everyone over the age of 16. Identity cards were valid for 10 years, had to be updated within a year in case of change of residence, and their renewal required paying a fee. Under the Vichy regime, in addition to the face photograph, the family name, first names, date and place of birth, the card included the national identity number managed by the national statistics INSEE, which is also used as the national service registration number, as the Social Security account number for health and retirement benefits, for access to court files and for tax purposes. Under the decree 55-1397 of October 22, 1955*[32]*[33] a revised non-compulsory card, the *carte nationale d'identité* (CNI) was introduced.

The law (Art. 78-1 to 78-6 of the French Code of criminal procedure (*Code de procédure pénale*))*[34] mentions only that during an ID check performed by police, gendarmerie or customs, one can prove his identity "by any means", the validity of which is left to the judgment of the law enforcement official. Though not stated explicitly in the law, an ID card, a driving licence, a passport, a visa, a *Carte de Séjour*, a voting card are sufficient according to jurisprudency. The decision to accept other documents, with or without the bearer's photograph, like a Social Security card, a travel card or a bank card, is left to the discretion of the law enforcement officer.

According to Art. 78-2 of the French Penal Procedure Code ID checks are only possible:*[35]

- alineas 1 & 2 : if you are the object of inquiries or investigations, have committed, prepared or attempted to commit an offence or if you are able to give information about it (*contrôle judiciaire*);*[36]
- alinea 4 : until 20 km from the French borders and in the ports, airports and railway stations open to international traffic (*contrôle aux frontières*);*[37]
- alinea 3 : whatever the person's behaviour, to prevent a breach of public order and in particular an offence against the safety of persons or property (*contrôle administratif*).*[38]

The last case allows checks of passers-by ID by the police, especially in neighborhoods with a higher criminality rate which are often the poorest at the condition, according to the *Cour de cassation*, that the policeman doesn't refer only to "general and abstract conditions" but to "particular circumstances able to caracterise a risk of breach of public order and in particular an offence against the safety of persons or property" (Cass. crim. 05/12/1999, n°99-81153, Bull., n°95).

In case of necessity to establish your identity, not being able to prove it "by any means"(for example the legality of a road traffic *procès-verbal* depends of it), may lead to a temporary arrest (*vérification d'identité*) of up to 4 hours for the time strictly required for ascertaining your identity according to art. 78-3 of the French Code of criminal procedure (*Code de procédure pénale*).*[34]

For financial transactions, ID cards and passports are almost always accepted as proof of identity. Due to possible forgery, driver's licenses are sometimes refused. For transactions by cheque involving a larger sum, two different ID documents are frequently requested by merchants.

The current identification cards are now issued free of charge and optional. The current government has proposed a compulsory biometric card system, which has been opposed by human rights groups and by the national authority and regulator on computing systems and databases, the *Commission nationale de l'informatique et des libertés*, CNIL. Another non-compulsory project is being discussed.

Germany Main article: German identity card

It is compulsory for all German citizens age 16 or older to

Specimen of a German identity card issued since November 2010.

possess either a *Personalausweis* (identity card) or a passport but not to carry one. Police officers and other officials have a right to demand to see one of those documents (obligation of identification); however the law does not state that one is obliged to submit the document at that very moment. But as driver's licences are not legally accepted forms of identification in Germany, people usually choose to carry their *Personalausweis* with them. Beginning in November 2010, German ID cards are issued in the ID-1 format and can also contain an integrated digital signature, if so desired. Until October 2010, German ID cards were issued in ISO/IEC 7810 ID-2 format. The cards have a photograph

and a chip with biometric data, including, optionally, fingerprints.

Gibraltar Main articles: Gibraltar identity card and History of nationality in Gibraltar

Gibraltar has operated an identity card system since 1943.

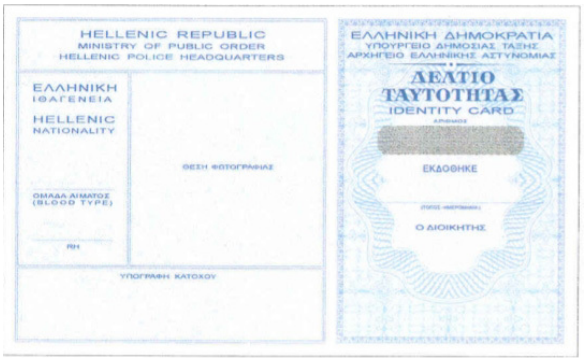
The cards issued were originally folded cardboard, similar to the wartime UK Identity cards abolished in 1950. There were different colours for British and non-British residents. Gibraltar requires all residents to hold identity cards, which are issued free.

In 1993 the cardboard ID card was replaced with a laminated version. However, although valid as a travel document to the UK, they were not accepted by Spain.

A new version in an EU compliant format was issued and is valid for use around the EU although as very few are seen there are sometimes problems in its use, even in the UK. ID cards are accepted financial transactions, but apart from that and to cross the frontier with Spain, they are not in common use.

Greece Main article: Greek identity card

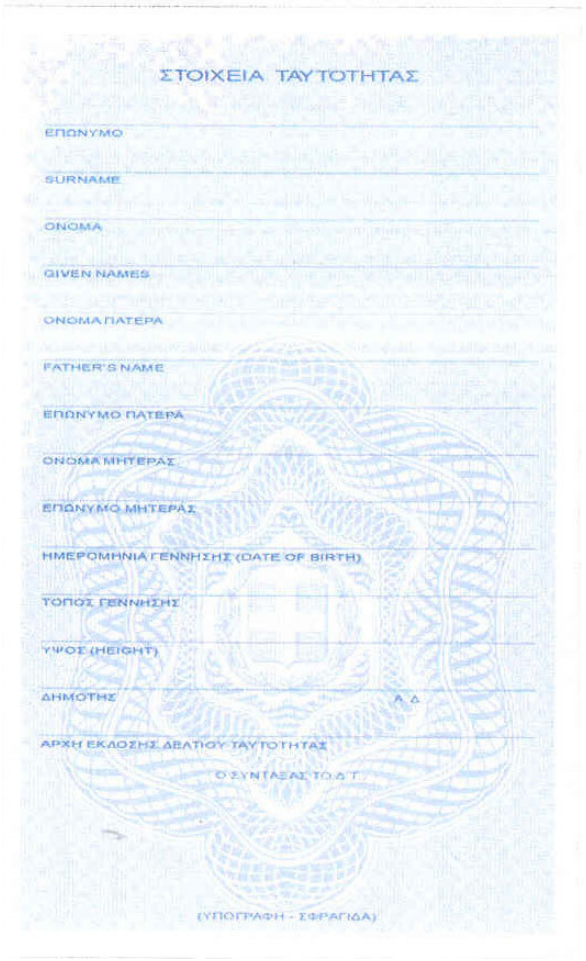
A compulsory, universal ID system based on personal ID



Greek ID card (front)

cards has been in place in Greece since World War II. ID cards are issued by the police on behalf of the Headquarters of the Police (previously issued by the Ministry of Public Order, now incorporated in the Ministry of Internal Affairs) and display the holder's signature, standardized face photograph, name and surname, father's name and surname, mother's name and maiden surname, date and place of birth, height, municipality, and the issuing police precinct. There are also two optional fields designed to facilitate emergency medical care: ABO and Rhesus factor blood typing.

Fields included in previous ID card formats, such as vocation or profession, religious denomination, domiciliary ad-



Greek ID card (back)

dress, name and surname of spouse, fingerprint, eye and hair color, citizenship and ethnicity were removed permanently as being intrusive of personal data and/or superfluous for the sole purpose of personal identification.

Since 2000, name fields have been filled in both Greek and Latin characters. According to the Signpost Service of the European Commission [reply to Enquiry 36581], old type Greek ID cards "are as valid as the new type according to Greek law and thus they constitute valid travel documents that all other EU Member States are obliged to accept." In addition to being equivalent to passports within the European Economic Area, Greek ID cards are the principal means of identification of voters during elections.

Since 2005, the procedure to issue an ID card has been automated and now all citizens over 12 years of age must have an ID card, which is issued within one work day. Prior to that date, the age of compulsory issue was at 14 and the whole procedure could last several months.

In Greece, an ID card is a citizen's most important state

document. For instance, it is required to perform banking transactions if the teller personnel is unfamiliar with the apparent account holder, to interact with the Citizen Service Bureaus (KEP),*[39] receive parcels or registered mail etc. Citizens are also required to produce their ID card at the request of law enforcement personnel.

All the above functions can be fulfilled also with a valid Greek passport (e.g. for people who have lost their ID card and have not yet applied for a new one, people who happen to carry their passport instead of their ID card or Greeks who reside abroad and do not have an identity card, which can be issued only in Greece in contrast to passports also issued by consular authorities abroad).

Hungary Main article: Hungarian identity card

Currently, there are three types of valid ID documents

Hungarian ID card (obverse).

Hungarian ID card (reverse).

(*Személyi igazolvány*, abbr. *Sz.ig.*) in Hungary: the oldest valid ones are hard-covered, multipage booklets and issued before 1989 by the People's Republic of Hungary, the second type is a soft-cover, multipage booklet issued after the change of regime; these two have one, original photo of the owner embedded, with original signatures of the owner and the local police's representative. The third type is a plastic card with the photo and the signature of the holder digitally reproduced. These are generally called Personal Identity Card.

The plastic card shows the owners full name, maiden name if applicable, birth date and place, mother's name, sex, the IDs validity period and the local state authority which issued the card. The card has a 6 number + 2 letter unique ID. It does not have any information about the owners residual address, nor his/her Personal ID – this sensitive information is contained on a separate card, called Authority ID. Personal IDs have been compulsory since 1975: it has the following format in numbers: sex (1 number) – birth date (6 numbers) – unique ID (4 numbers). It is no longer used as a personal identification number, but as a statistical signature.

Other valid documents are the passport (blue colored or red colored with RFID chip) and the driving license; an individual is required to have at least one of them on hand all the time. The Personal Identity Card is mandatory to vote in state elections or open a bank account in the country.

ID cards are issued to permanent residents of Hungary; if he is a foreign citizen, the card has a different color.

Ireland The Republic of Ireland does not have an official identity card.

Italy See also: Italian electronic identity card

All Italian citizens are entitled to request an identity card which would be issued by the municipality in which they live. The card lasts ten years and is a valid document to leave the country when travelling to another EU country.*[40] It is not compulsory to carry the card itself, as the authorities only have the right to ask for the identity of a person, not for a specific document. However, if public-security officers are not convinced of the claimed identity, such as may be the case for a verbally provided identity claim, they may keep the claimant in custody until his/her identity is ascertained;*[41] such an arrest is limited to the time necessary for identification and has no legal consequence.

A classic Italian identity card (now in the process of being replaced by a newer template) has four pages, containing:

1. Issuing municipality, card number and owner's name and surname;
2. Owner's name, surname, birth date and place, citizenship, city of residence, address, civil status (optional) and profession; in addition, physical features such as height, hair and eye color, and any other particular feature not visible from the photo (e.g. having a twin or being an amputee) can be noted;

Italian classic ID card, front page

3. Photo and signature of the owner, date of issue and stamp of the issuing municipality.
4. Expiration date and card number.

A field for fingerprints has been present for a long time at the bottom of the third page, but is rarely if ever used. Also, physical features are normally not measured rigorously, but are just verbally asked to the applicant (such as height) or quickly ascertained by administrative personnel on the spot, with no checks for hair dying or cosmetic lenses.

The classic Italian ID card is made of paper, not plastic, and its lamination with plastic pouches is explicitly forbidden, because it would interfere with the anti-forging heat sensitive pattern on the back of the card (see reference).*[42] Lamination of ID cards was popular and widely practised until the current prohibition was introduced, because of the low quality of the employed paper, which tends to break apart after a few months in a wallet. Removable pouches are often employed to limit damage, but the odd size of the card (about 1 cm larger than a plastic credit card in both directions) makes it difficult to store it easily in a wallet. Furthermore, the usage of paper makes the card easy to forge, and foreign countries outside the EU sometimes refuse to accept it as a valid document. These common criticism were considered in the development of the Italian electronic identity card, which is in the more common credit-card format.

All foreigners in Italy are required by law to have an ID with them at all times.*[43] Citizens of EU member countries must be always ready to display an identity document that is legally government-issued in their country. Non-EU residents must have their passport with customs entrance stamp or a residence permit issued by Italian authorities; while all the resident/immigrant aliens must have a residence permit (otherwise they are illegal and face deportation), foreigners from certain non-EU countries staying in Italy for a limited amount of time (typically for tourism) may be only required to have their passport with proper customs stamp. Additionally permanently resident foreigners can ask to be issued an Italian ID card by the local authorities of their city/town of residence.

Netherlands See also: Dutch identity card and Dutch passport

Dutch citizens from the age of 14 are required to be able to show a valid identity document upon request by a police officer or similar official. Furthermore, identity documents are required when opening bank accounts and upon start of work for a new employer. Official identity documents for residents in the Netherlands are:

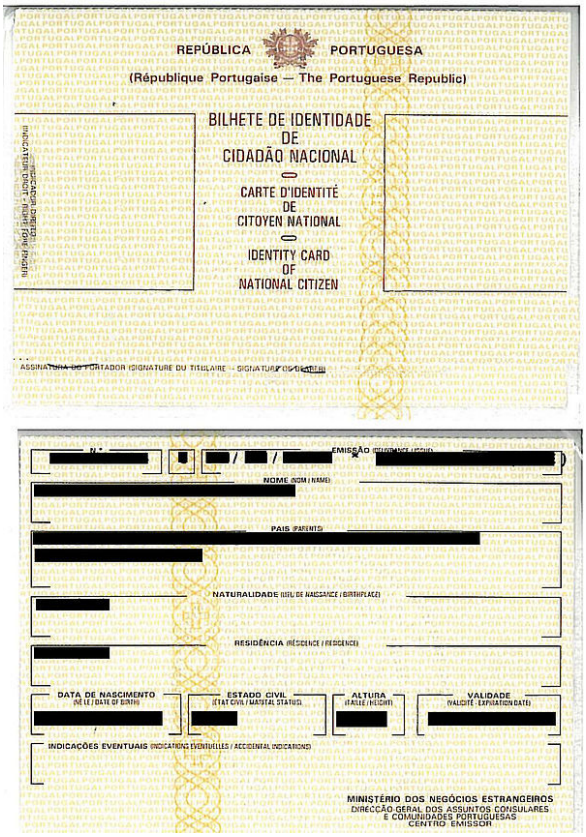
- Dutch passport
- Dutch identity card
- Alien's Residence permit
- *Geprivilegieerdenkaart* (amongst others for the corps diplomatique and their family members)
- Passports/national ID cards of members of other E.E.A. countries

For the purpose of identification in public (but not for other purposes), also a Dutch driving license often may serve as an identity document. In the Caribbean Netherlands, the Dutch Identity Card is not valid; and the Identity card BES is an obligatory document for all residents.

Poland Main article: Polish National Identity Card

Every Polish citizen 18 years of age or older residing permanently in Poland must have an Identity Card (Dowód osobisty) issued by the local Office of Civic Affairs. Polish citizens living permanently abroad are entitled, but not required, to have one.

Polish national ID card (front and back)



Old format of the Portuguese national ID card (front and back)

Portugal Main article: Citizen Card (Portugal)

All Portuguese citizens are required by law to obtain an Identity Card as they turn 6 years of age. They are not required to carry with them always but are obligated to present them to the lawful authorities if requested. The old format of the cards (yellow laminated paper document) featured the photo, the fingerprint, and the name of parents, among other information. It is currently being replaced by grey plastic cards with a chip, called *Cartão de Cidadão* (Citizen's Card), which now incorporate NIF (Tax Number), Cartao de Utente (Health Card) and Social Security, all of which are protected by a PIN obtainted when the card was successfully taken into possession

Characteristics The new Citizen's Card is technologically more advanced than the former Identity Card and therefore enjoys the following characteristics:

- From the **physical point of view** the Citizen's Card will have a 'smart card' format and will replace the existing Identity Card, taxpayer card, Social Security card, voter's card and National Health Service user's card.
- From the **visual point of view** the front of the card will display the holder's photograph and basic personal details. The back will list the numbers under which the holder is registered with the different bodies whose cards the Citizen's Card combines and replaces. The back will also contain an optical reader and the chip.
- From the **electronic point of view** the card will have a contact chip, with digital certificates (for electronic authentication and signature purposes). The chip may also hold the same information as the physical card itself, together with other data such as the holder's address.

Romania Main article: Romanian identity card

Every citizen of Romania must register for an ID card (**Carte de identitate**, abbreviated **CI**) at the age of 14. The CI offers proof of the identity, address, sex and other data of the possessor. It has to be renewed every 10 years. It can be used instead of a passport for travel inside the European Union and several other countries outside the EU.

Another ID Card is the Provisional ID Card (**Cartea de Identitate Provizorie**) issued temporarily when an individual cannot get a normal ID Card. Its validity extends for up to 1 year.

Specimen of a Romanian identity card issued since 2009.

Other forms of officially accepted identification include the driver's license and the birth certificate. However, these are accepted only in limited circumstances and cannot take the place of the ID Card in most cases. The ID Card is mandatory for dealing with government institutions, banks or currency exchange shops. A valid passport may also be accepted, but usually only for foreigners.

In addition, citizens can be expected to provide the personal identification number (CNP) in many circumstances; purposes range from simple unique identification and internal book-keeping (for example when drawing up the papers for the warranty of purchased goods) to being asked for identification by the police. The CNP is 13 characters long, with the format S-YY-MM-DD-RR-XXX-Y. Where S is the sex, YY is year of birth, MM is month of birth, DD is day of birth, RR is a regional id, XXX is a unique random number and Y is a control digit.

Presenting the ID Card is preferred but not mandatory when asked by police officers; however, in such cases people are expected to provide a CNP or alternate means of identification which can be checked on the spot (via radio if needed).

The information on the ID Card is required to be kept updated by the owner; current address of domicile in particular. Doing otherwise can expose the citizen to certain fines or be denied service by those institutions that require a valid, up to date Card. In spite of this, it is common for people to let the information lapse or go around with expired ID Cards.

A new electronic ID Card is under project of implementation and should be fully implemented by 2014.

Slovakia The Slovak ID card (Slovak: *Občiansky preukaz*) is a picture ID in Slovakia. It is issued to citizens of Slovak Republic who are 15 or older. A Slovak ID card is officially recognised by all member states of the European Union for travel within the EU. For travel outside the EU, Slovak citizens may also require a passport, which is a legally accepted form of picture ID as well. Police officers and some other officials have a right to demand to see one of those documents, and the law states that one is obliged to submit such a document at that very moment. If one fails to comply, law enforcement officers are allowed to insist on personal identification at the police station.

Slovak ID card (front and back) New EU template

Slovenia Every Slovenian citizen regardless of age has the right to acquire an Identity Card (Slovene: *Osebna izkaznica*) where every citizen of the Republic of Slovenia of 18 years of age or older is obliged by law to acquire one and carry it at all times (or any other Identity document with a picture i.e. Slovene Passport). The Card is a valid Identity Document within all members states of the European Union for travel within the EU. With exception of the Faroe Islands and Greenland, though it may be used to travel outside of the EU: Norway, Liechtenstein, BiH, Macedonia, Montenegro, Serbia, Switzerland. The front side displays the name and surname, sex, nationality, date of birth and expiration date of the card, as well as the number of the ID card a black and white photograph and a signature. On the back, permanent address, administrative unit, date of issue, EMŠO, and a code with key information in a machine-readable zone. Depending on the holders age (and some-

times also other factors), the card had a validity of 5 years or 10 years, and 1 year for foreigners living in Slovenia.

In Slovenia the ID cards importance is equaled only by the Slovenian passport, but a due to size a lot more practical.

Specimen of a Spanish DNI *card.(1991-2006)*

Spain In Spain, citizens, resident foreigners and companies have similar but distinct identity numbers, some with prefix letters, all with a check-code*[44]

- **NIF** Both natural and legal persons have a tax code or *Número de Identificación Fiscal* (NIF) which is the same as their identity document. For companies, this was formerly known as *Código de Identificación Fiscal* (CIF)
- **DNI** Spanish Citizens have a *Documento Nacional de Identidad* (DNI) that bears this number without any letter prefix. This is sometimes known by obsolete names such as *Cédula de Ciudadanía* (CC),*Carné de Identidad* (CI) or *Cédula de Identidad* (CI)

  Spanish citizens under 14 may, but over 14 must acquire a National Identity Card *(DNI)*. It is issued by the National Police formerly ID-1 (bank-card) format paper encapsulated in plastic. Since 2006 a new version of the 'DNI' is being introduced. The new 'Electronic DNI' is a Smart card that allows for digital signing of documents. The chip contains most of the personal information, which is printed on the card, as well as a digitized version of the bearer's face, signature and finger prints.*[45]

  On the front there is a photograph, the name and two surnames (see Spanish naming customs), the bearer's signature, an id number, the issue date and the expiration date. On the reverse appears the birth date and place, the gender, both parents' names (if known), and the current address. At the bottom, key information is present in a machine-readable zone. Depending on holder's age, the card has a validity of 5 years, 10 years or indefinite (for the elderly).*[46]

- **CIF** *Código de Identidad Fiscal* has been retained only for associations and foundation have a CIF which starts with the letter -G
- **NIE** Foreigners (e**X**tranjeros in Spanish) are issued with a Número de identificación Español which starts with the letter X These were similar to DNI cards, but are now security printed A4 format. NIE cards for EU citizens have been abolished.

Despite the NIF/CIF/NIE/NIF distinctions the *identity number* is unique and always has eight digits followed by a letter calculated from a 23-Modular arithmetic check used to verify the correctness of the number. The letters I, Ñ, O, U are not used and the sequence is as follows:

This number is the same for tax, social security and all legal purposes. Without this number (or a foreign equivalent such as a passport number) a contract may not be enforceable.

In Spain, the formal identity number on an ID card is the most important piece of identification. It is used in all public and private transactions. It is required to open a bank account, to sign a contract, to have state insurance, to register in a university and should be shown when being fined by a police officer.*[47] It is one of the official documents required to vote at any election, although any other form of official ID such as a driving licence or passport may be used. The card also constitutes a valid travel document within the European Union.*[48]

Non-resident citizens of countries such as the United Kingdom, where passport numbers are not fixed for the holder's life but change with renewal may experience difficulty with legal transactions after the document is renewed since the old number is no longer verifiable on a valid (foreign) passport.

Sweden Main article: Identity documents in Sweden

Sweden does not have a legal statute for compulsory identity documents. However ID-cards are regularly used to ascertain a person's identity when completing certain transactions. These include but are not limited to banking and age verification. Also interactions with public authorities often require it, in spite of the fact that there is no law explicitly requiring it, because there are laws requiring authorities to somehow verify people's identity. Without Swedish identity documents difficulties can occur accessing health care services, receiving prescription medications and getting salaries or grants. From 2008, EU passports have been accepted for these services due to EU legislation (with exceptions including banking), but non-EU passports are not accepted. Identity cards have therefore become an important part of everyday life.

There are currently three public authorities that issue ID-cards. The tax office (Skatteverket), the Police and the transport board.

The tax office cards can only be used within Sweden to validate a persons identity, but they can be obtained both by Swedish citizens and those that currently reside in Sweden. A Swedish personal identity number is required. It is possible to get one without having any Swedish id-card. In this case a person holding such a card must guarantee the identity, and the person must be a verifiable relative or the boss at the company the person has been working or a few other verifiable people.

The Police can only issue identity documents to Swedish citizens. They issue an internationally recognised id-card according to EU standard usable for intra-Schengen travel, and Swedish passports which are acceptable as identity documents inside the EU.*[49]

The Transport board issues driving licences which are valid as identity documents in Sweden. To obtain one, one must be approved as a driver and strictly have another Swedish identity document as proof of identity.

In the past there have been certain groups that have experienced problems obtaining valid identification documents. This was due to the initial process that was required to validate one's identity, unregulated security requirements by the commercial companies which issued them. Since July 2009, the tax office has begun to issue identity cards and this has simplified the identity validation process for foreign passport holders. Still there are requirements for the identity validation that can cause trouble especially for foreign citizens but the list of people who can validate one's identity has been extended.

United Kingdom Main article: Identity Cards Act 2006
See also: Identity Documents Act 2010

The UK had an identity card during World War II as part of a package of emergency powers invoked and was abolished soon after. Identity cards were first proposed in the mid-1980s for people attending football matches, following a series of high profile hooliganism incidents involving English football fans. However, this proposed identity card scheme never went ahead as Lord Taylor of Gosforth ruled it out as "unworkable" in the Taylor Report of 1990.

By 2006 several groups such as No2ID had formed to campaign against ID cards in Britain. The UK Labour government progressively introduced compulsory identity cards for non-EU residents in Britain starting late 2008. After the 2010 general election a new government was formed, comprising a coalition between two parties that had pledged to scrap ID cards - the Conservatives and Liberal Democrats - and the Home Office announced that the national identity register had been destroyed on 10 February 2011.*[50]

Identity cards for British nationals were introduced in 2009 on a voluntary basis. Only workers in certain high-security professions, such as airport workers, were required to have an identity card, and this general lack of ID being compulsory tends to remain the case today.

Driving licences, particularly the photocard driving licence introduced in 1998, and passports are now the most widely used ID documents in the United Kingdom, but the former cannot be used as travel documents, for example for travel to other EEA countries. However, driving licences from the UK and other EU countries are usually accepted within other EEA countries for identity verification. Given that passports do not fit in a typical wallet or purse, most people do not carry their passports in public without an advance knowledge that they are going to need them. For people from the UK and other countries where national id cards are not used or not common, this leaves driving licences as the only valid form of ID to be presented, if requested by an authority for a legitimately-given reason, but unlike a travel document, they do not show the holder's nationality or immigration status. Colloquially, in day-to-day life, most authorities do not ask for identification from individuals in a sudden, spot check type manner, such as by police or security guards, although this may become a concern in instances of stop and search.

There are also various PASS-accredited cards, used mainly for proof-of-age purposes, but they are not very commonly carried amongst people.

Non-European Union

Albania Main article: Albanian Identity Card

From January 12, 2009 the Government of Albania is issu-

Albanian electronic ID Card 2009

ing a compulsory electronic and biometric ID Card *(Letërnjoftim)* for its citizens.*[51] Every citizen at age 16 must apply for Biometric ID card.

Belarus Main article: Belarusian passport

Belarus has combined the international passport and the internal passport into one document which is compulsory from age 16. It follows the international passport convention but has extra pages for domestic use.

Bosnia and Herzegovina Main article: Bosnian-Herzegovinian identity card

Bosnia and Herzegovina allows every person over the age

Bosnian-Herzegovinian identity card

of 15 to apply for an ID card, and all citizens over the age of 18 must have the national ID card with them at all times. A penalty is issued if the citizen does not have the acquired ID card on them or if the citizen refuses to show proof of identification.

Iceland The Icelandic state-issued identity cards are called "Nafnskírteini". Most people use driver's licences instead. Identity documents are not mandatory to carry by law (unless driving a car), but can be needed for bank services, age verification and other situations.

The Macedonian identity card

Macedonia Main article: Macedonian identity card

The Macedonian identity card (Macedonian: Лична карта, Lična karta) is a compulsory identity document issued in the Republic of Macedonia. The document is issued by the police on behalf of the Ministry of Interior. Every person over 18 can get and must get an identity card.

Moldova Main article: Moldovan Identity Card

In Moldova Identity Cards (Romanian: *Buletin de identitate*) are being issued since 1996. The first person to get identity card was former president of Moldova - Mircea Snegur. Since then all the Moldovan citizens are required to have and use it inside the country. It can't be used to travel outside the country, however it is possible to pass so-called Transnistrian border with it.

The Moldovan Identity card may be obtained by a child from his/her date of birth. State company "Registru" is responsible for issuing Identity cards and for storing data of all Moldovan citizens.

Monaco Main article: Monégasque identity card

Monégasque identity cards are issued to Monégasque citizens and can be used for travel within the Schengen Area.

Montenegro Main article: Montenegrin identity card

Montenegrin national ID card

In Montenegro every resident citizen over the age of 14 can have their *Lična karta* issued, and all persons over the age of 18 must have ID cards and carry them at all times when they are in public places. It can be used for international travel to Bosnia and Herzegovina, Serbia, Macedonia, Kosovo and Albania instead of the passport.

Norway In Norway there is no law penalising non possession of an identity document. But there are rules requiring it for services (or other identification method such as personal recognition etc.) like banking and voting. The following documents are generally considered valid (varying a little, since no law lists them):*[52] Nordic driving licence, passport (often only from EU), national id card from EU, Norwegian ID card from banks and some more. But there is no ID card for anyone except bank ID card (normally printed on the reverse of a credit card). To get a bank ID card either a Nordic passport or another passport together with Norwegian residence and work permit is needed. There is an ongoing plan to introduce a national ID card accrediting Norwegian citizenship, usable for travel within the EU, and for general identification. The plan started in 2007 and has been delayed several times and is now scheduled for 2016. Banks are campaigning to be freed from the task of issuing ID cards, stating that it the responsibility of state authorities.*[53] Some banks have already ceased issuing ID cards, so people need to bring their passport for e.g. offline credit card purchases if not in possession of a driving licence.*[54]

Russia Main article: Internal passport of Russia

- Domestic Passport front page
- Domestic Passport Data and Signature page

The role of identity document is primarily played by the so-called Russian internal passport, a passport-size booklet which contains a person's photograph, birth information and other data such as registration at the place of residence (informally known as propiska), marital data, information about military service and underage children. Internal passports are issued by the Federal Migration Service to all citizens who reach their 14th birthday and do not reside outside Russia. They are re-issued at the age 20 and 45.

The internal passport is commonly considered the only acceptable ID document in governmental offices, banks, while traveling by train or plane, getting a subscription service, etc. If the person does not have an internal passport (i.e. foreign nationals or Russian citizens who live abroad), an international passport can be accepted instead, theoretically in all cases. Another exception is army conscripts, who produce the Identity Card of the Russian Armed Forces.

Internal passports can also be used to travel to Ukraine, Belarus, Kazakhstan, Tajikistan, Kyrgyzstan, Abkhazia and South Ossetia.

Other documents, such as driving licenses or student cards, can sometimes be accepted as ID, subject to regulations.

Serbian national ID card

Serbia Main article: Serbian identity card

In Serbia every resident citizen over the age of 10 can have their *Lična karta* issued, and all persons over the age of 16 must have ID cards and carry them at all times when they are in public places.*[55] It can be used for international travel to Bosnia and Herzegovina, Montenegro and Macedonia instead of the passport.*[56] Contact microchip on ID is optional.

Kosovo issues its own identity cards. These documents are accepted by Serbia when used as identification while crossing the Serbia-Kosovo border/boundary.*[57] They can also be used for international travel to Montenegro*[58] and Albania.*[59]

Turkey Main article: Turkish identity card

The Turkish national ID card (Turkish: *Nüfus Cüzdanı*) is compulsory for all Turkish citizens from birth. Cards for males and females have a different colour. The front shows the first and last name of the holder, first names of both parents, birth date and place, and an 11 digit ID number. The back shows marital status, religious affiliation, the region of the country of origin, and the date of issue of the card. On February 2, 2010 the European Court of Human Rights ruled in a 6 to 1 vote that the religious affiliation section of the Turkish identity card violated articles 6, 9, and 12 of the European Convention of Human Rights, to which Turkey is a signatory. The ruling should coerce the Turkish government to completely omit religious affiliation on future identity cards. The Turkish police are allowed to ask any person to show ID, and refusing to comply may lead to arrest. It can be used for international travel to Northern Cyprus and Georgia (country) instead of a passport.

Ministry of Interior of Turkey is still working for release an EU-like identity cards for all Turkish citizens. New identity cards will be biometric as well as passport, and can be used as bank card, bus ticket or at international trips.

11.3.4 North America

Canada

In Canada, different forms of identification documentation are used, but there is no de jure national identity card. The Canadian passport is issued by the federal (national) government, and the provinces and territories issue various documents which can be used for identification purposes. The most commonly used forms of identification within Canada are the driver's licence and health care cards issued by provincial and territorial governments. The widespread usage of these two documents for identification purposes has made them de facto identity cards.

In Canada, a driver's licence usually lists the name, home address, and date of birth of the bearer. A photograph of the bearer is usually present, as well as additional information, such as restrictions to the bearer's driving licence. The bearer is required by law to keep the address up to date.

A few provinces, such as Québec and Ontario, issue provincial health care cards which contain identification information, such as a photo of the bearer, their home address, and their date of birth. British Columbia and Ontario are among the provinces that produce photo identification cards for individuals who do not possess a driving licence, with the cards containing the bearer's photo, home address, and date of birth.

For travel abroad, a passport is almost always required. There are a few minor exceptions to this rule, with these exceptions mainly applying to international travel within North America, such as the NEXUS programme and the Enhanced Drivers License programme implemented by a few provincial governments as a pilot project. These programmes have not yet gained widespread acceptance, and the Canadian passport remains the most useful and widely accepted international travel document.

Costa Rica

Every Costa Rican citizen must carry an identity card after turning 18. The card is named *Cédula de Identidad* and it is issued by the local registrar's office (*Registro Civil*), an office belonging to the local elections committee (*Tribunal Supremo de Elecciones*), which in Costa Rica has the same rank as the Supreme Court. Each card has a unique number composed of nine numerical digits, the first of them being the province where the citizen was born (with other significance in special cases such as granted citizenship to foreigners, adopted persons or in rare cases with old people where no birth certificate was processed at birth); after this digit, two blocks of four digits follow; the combination corresponds to the unique identifier of the citizen.

It is widely requested as part of every legal and financial purpose, often requested at payment with credit or debit cards for identification guarantee and requested for buying alcoholic beverages or cigarettes or upon entrance to adults-only places like bars.

The card must be renewed every ten years and is freely issued again if lost. Among the information included there are, on the front, two identification pictures and digitized signature of the owner, identification number (known colloquially just as the *cédula*), first name, first and second-last names and an optional *known as* field. On the back, there is again the identification number, birth date, where the citizen issues its vote for national elections or referendums, birthplace, gender, date when it must be renewed and a matrix code that includes all this information and even a digitized fingerprint of the thumb and index finger.

The matrix code is not currently being used nor inspected by any kind of scanner.

Besides this identification card, every vehicle driver must carry a driving licence, an additional card that uses the same identification number as the ID card (Cédula de Identidad) for the driving license number. A passport is also issued with the same identification number used in the ID card. The same situation occurs with the Social Security number; it is the same number used for the ID card.

All non-Costa Rican citizens with a *resident status* must

carry an ID card (*Cédula de Residencia*), otherwise, a passport and a valid visa. Each resident's ID card has a unique number composed of 12 digits; the first three of them indicate their nationality and the rest of them a sequence used by the immigration authority (called Dirección General de Migración y Extranjería). As with the Costa Rican citizens, their Social Security number and their driver's license (if they have it) would use the same number as in their own resident's ID card.

Dominican Republic

A "Cédula de Identidad y Electoral" (Identity and Voting Document) is a National ID that is also used for voting in both Presidential and Congressional ballots. Each "Cédula de Identidad y Electoral" has its unique serial number composed by the serial of the municipality of current residence, a sequential number plus a verification digit. This National ID card is issued to all legal residents of adult age. It is usually required to validate job applications, legally binding contracts, official documents, buying/selling real estate, opening a personal bank account, obtaining a Driver's License and the like. It is issued free of charge*[60] by the "Junta Central Electoral" (Central Voting Committee) to all Dominicans not living abroad at the time of reaching adulthood (16 years of age) or younger is they are legally emancipated. Foreigners that have taken permanent residence and have not yet applied for Dominican naturalization (i.e. have not opted for Dominican citizenship but have taken permanent residence) are required to pay an issuing tariff and must bring along their non-expired Country of Origin passport, deposit photocopies of their Residential Card and Dominican Red Cross Blood Type card. Foreigners residing on a permanent basis must renew their "Foreign ID" on a 2, 4 or 10-year renewal basis (about US$63 - US$240, depending on desired renewal period).*[61]

El Salvador

In El Salvador, ID Card is called Documento Único de Identidad (DUI) (Unique Identity Document). Every citizen above 18 years must carry this ID for identification purposes at any time. It is not based on a smartcard but on a standard plastic card with two-dimensional bar-coded information with picture and signature.

Guatemala

In January 2009, the National Registry of Persons (RENAP) in Guatemala began offering a new identity document in place of the *Cédula de Vecindad* (neighborhood identity document) to all Guatemala citizens and foreigners. The new document is called "Documento Personal de Identification" (DPI) (Personal Identity Document). It is based on a smartcard with a chip and includes an electronic signature and several measures against fraud.

Mexico

Not mandatory, but needed in almost all official documents, the CURP is the standardized version of an identity document. It actually could be a printed green wallet-sized card or simply an 18-character identification key printed on a birth or death certificate.*[62]

Unlike most other countries, Mexico has assigned a CURP to nearly all minors, since both the government and most private schools ask parents to supply their children's CURP to keep a data base of all the children. Also, minors must produce their CURP when applying for a passport or being registered at Public Health services by their parents.

Most adults need the CURP code too, since it is required for almost all governmental paperwork like tax filings and passport applications. Most companies ask for a prospective employee's CURP, voting card, or passport rather than birth certificates.

To have a CURP issued for a person, a birth certificate or similar proof must be presented to the issuing authorities to prove that the information supplied on the application is true. Foreigners applying for a CURP must produce a certificate of legal residence in Mexico. Foreign-born Mexican naturalized citizens must present their naturalization certificate. On 21 August 2008 the Mexican cabinet passed the National Security Act, which compels all Mexican citizens to have a biometric identity card, called Citizen Identity Card (*Cédula de identidad ciudadana*) before 2011.

On February 13, 2009 the Mexican government designated the state of Tamaulipas to start procedures for issuing a pilot program of the national Mexican ID card.

Although the CURP is the *de jure* official identification document in Mexico, the Federal Electoral Institute's voting card is the *de facto* official identification and proof of legal age for citizens of ages 18 and older.

On July 28, 2009 Mexican President Felipe Calderón, facing the Mexican House of Representatives, announced the launch of the Mexican national Identity card project, which will see the first card issued before the end of 2009.

United States

Main article: Identity documents in the United States

For most people, driver's licenses issued by the respective

state and territorial governments have become the *de facto* identity cards, and are used for many identification purposes, such as when purchasing alcohol and tobacco, opening bank accounts, and boarding planes. Individuals who do not drive are able to obtain an identification card with the same functionality from the same state agency that issues driver's licenses. In addition, many schools issue student and teacher ID cards.*[63]

The United States passed a bill entitled the REAL ID Act on May 11, 2005. The bill compels states to begin redesigning their driver's licenses to comply with federal security standards by December 2009. Federal agencies would reject licenses or identity cards that do not comply, which would force Americans accessing everything from airplanes to national parks and courthouses to have the federally mandated cards. At airports, those not having compliant licenses or cards would simply be redirected to a secondary screening location. The REAL ID Act is highly controversial, and with 25 states have approved either resolutions or binding legislation not to participate in the program, and with President Obama's selection of Janet Napolitano (a prominent critic of the program) to head the Department of Homeland Security, the future of the law remains uncertain,*[64] and bills have been introduced into Congress to amend or repeal it.*[65] The most recent of these, dubbed PASS ID, would eliminate many of the more burdensome technological requirements but still require states to meet federal standards in order to have their ID cards accepted by federal agencies.

The bill takes place as governments are growing more interested in implanting technology in ID cards to make them smarter and more secure. In 2006, the U.S. State Department studied issuing passports with Radio-frequency identification, or RFID, chips embedded in them. Virginia may become the first state to glue RFID tags into all its driver's licenses. Seventeen states, however, have passed statutes opposing or refusing to implement the Real ID Act.*[66]

Since February 1, 2008, U.S. citizens may apply for passport cards, in addition to the usual passport books. Although their main purpose is for land and sea travel within North America, the passport card may also be accepted by federal authorities (such as for domestic air travel or entering federal buildings), which may make it an attractive option for people residing where state driver's licenses and I.D. cards are not REAL ID-compliant, should those requirements go into effect. TSA regulations list the passport card as an acceptable identity document at airport security checkpoints.*[67]

U.S. Citizenship and Immigration Services has indicated that the U.S. Passport Card may be used in the Employment Eligibility Verification Form I-9 (form) process.*[68] The passport card is considered a "List A" document that may be presented by newly hired employees during the employment eligibility verification process to show work authorized status. "List A" documents are those used by employees to prove both identity and work authorization when completing the Form I-9.

The passport card can be used as a valid proof of citizenship and proof of identity both inside and outside the United States.*[69]

11.3.5 Oceania

Australia

Australia does not have an identity card. There have been two proposals to introduce ID cards for tax and social security access in Australia: The Australia Card in 1985 by the Hawke Labor Government and the Health and Social Services Access Card in 2006 by the Howard Liberal Government. Although neither card would have been an official compulsory ID card, they were both criticised as leading to *de facto* ID cards. Ultimately, both proposals failed.

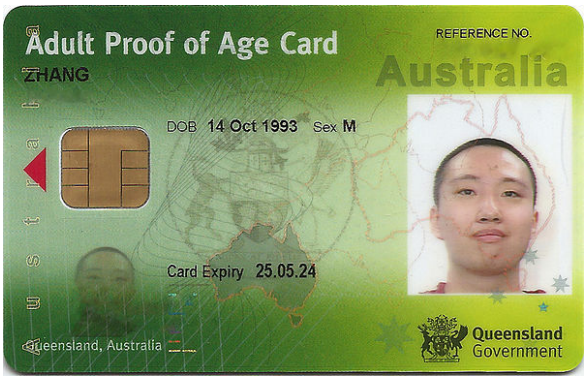
Instead, various identity documents are used or required to prove a person's identity, whether for government or commercial purposes.

A driver licence is the widely accepted form of identification in Australia.

Currently, driver licences are issued by the States and territories and are the most widely used personal identification document. Driver licences list a person's full name, date of birth, current address and contains a photograph. It can commonly be used for personal identification for various purposes such as obtaining various government permits and documentation (for example, passport or tax file number) as well as for opening bank accounts or applying for credit cards.

It is the *de facto* identity card in Australia.

For people who do not drive, the road authorities will issue a "Photo Card", also called "Proof of Age Card". In



A Proof of Age Card ("Photo Card") issued in Queensland.

some states, like New South Wales, Photo Card can be only issued to people who do not have a driver licence, but in some states, like Queensland, it can be issued to people who have a driver licence as another type of identity.

Identification indicating age is commonly required to purchase alcohol and tobacco and to enter nightclubs and gambling venues. For those persons over 18 who do not have a driver licence or passport, State governments provide 18+ Cards as proof of age. It is also available to people who do not wish to use a driver licence.* [70]

Other important identity documents include a passport, an official birth certificate, an official marriage certificate, cards issued by government agencies (typically social security cards), some cards issued by commercial organisations (e.g. a debit or credit card), and utility accounts. Often, some combination of identity documents is required, such as an identity document linking a name, photograph and signature (typically photo-ID in the form of a driver licence or passport), evidence of operating in the community, and evidence of a current residential address.

New Zealand

Legal forms of identification are used mainly for purchase of alcohol and cigarettes and entry to nightclubs. They can also be required for the purchase of spray paint and glues, and for some bank transactions. Forms of legal identification are New Zealand and overseas passports, New Zealand drivers' licenses and 18+ cards from the Hospitality Association of New Zealand. Overseas drivers' licenses may not be sufficient for the purchase of alcohol and tobacco. Firearms licences are a form of photo identification issued by the New Zealand Police.

Current front side of Argentine DNI Card

11.3.6 South America

Argentina

Main article: Documento Nacional de Identidad (Argentina)

Documento Nacional de Identidad or DNI(which means National Identity Document) is the main identity document for Argentine citizens. It is issued at a person's birth, and updated at 8 and 14 years of age simultaneously in one format: a card (DNI tarjeta); it is valid if identification is required, and is required for voting. They are produced at a special plant by the Argentine national registry of people (ReNaPer).* [71]

Brazil

Main article: Brazilian Identity Card

In Brazil, at the age of 18, all Brazilian citizens are supposed to be issued a *cédula de identidade* (ID card), usually known by its number, the *Registro Geral (RG)*, Portuguese for "General Registry". The cards are needed to obtain a job, to vote, and to use credit cards. Foreigners living in Brazil have a different kind of ID card. Since the RG is not unique, being issued in a state-basis, in many places the CPF (the Brazilian revenue agency's identification number) is used as a replacement. The current Brazilian driver's license contains both the RG and the CPF, and as such can be used as an identification card as well.

There are plans in course to replace the current RG system with a new *Registro de Identidade Civil* (Civilian Identity Registry), which will be national in scope, and to change the current ID card with a new smartcard.

Colombia

Every resident of Colombia over the age of 14 must bear an identity card (*Tarjeta de Identidad*). Upon turning 18 every resident must obtain a *Cédula de Ciudadanía*, which is the only document that proves the identity of a person for legal purposes. ID cards must be carried at all times and must be presented to the police or military upon request. If the individual fails to present the ID card upon request by the police or the military, he/she is most likely going to be detained for 24 hours at a UPJ (Unidad Permanente de Justicia) even if he/she is not a suspect of any wrongdoing. ID cards are needed to obtain employment, open bank accounts, obtain a passport, driver's license, military card, to enroll in educational institutions, vote or enter public buildings including airports and courthouses. Failure to produce ID is a misdemeanor punishable with a fine.

ID duplicate costs must be assumed by citizens.

Chile

Every resident of Chile over the age of 18 must have and carry at all times their ID Card called *Cédula de Identidad* issued by the Civil Registry and Identification Service. It contains the full name, gender, nationality, date of birth, photograph of the data subject, right thumb print, ID number, and personal signature.

This is the only official form of identification for residents in Chile and is widely used and accepted as such. It is necessary for every contract, most bank transactions, voting, driving (along with the driver's licence) and other public and private situations.

Peru

In Peru, it is mandatory for all citizens over the age of 18, whether born inside or outside the territory of the Republic, to obtain a **National Identity Document** (*Documento Nacional de Identidad*). The DNI is a public, personal and untransferable document.

The **DNI** is the only means of identification permitted for participating in any civil, legal, commercial, administrative, and judicial acts. It is also required for voting and must be presented to authorities upon request. The DNI can be used as a passport to travel to all South American countries that are members of UNASUR.

The DNI is issued by the National Registry of Identification and Civil Status (RENIEC). For Peruvians abroad, service is provided through the Consulates of Peru, in accordance with Articles 26, 31 and 8 of Law No. 26,497.

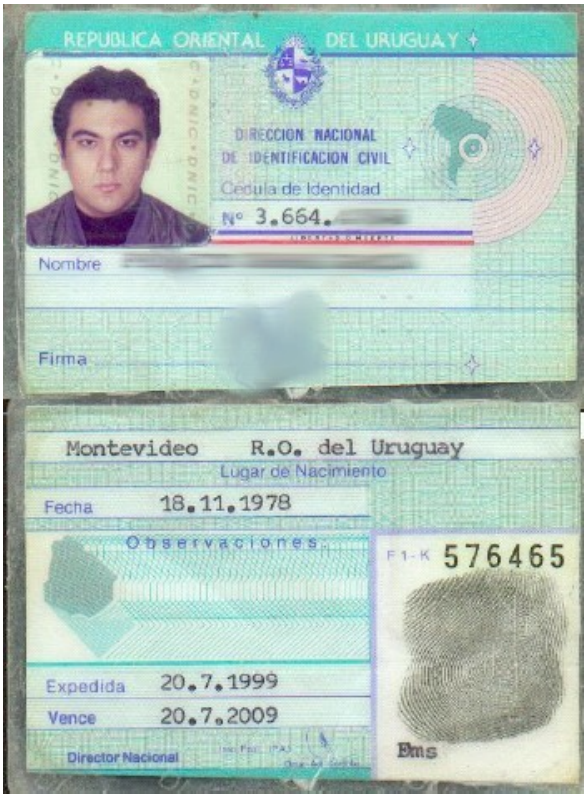
The document is card-sized as defined by ISO format ID-1 (prior to 2005 the DNI was size ISO ID-2; renewal of the card due to the size change was not mandatory, nor did previously-emitted cards lose validity). The front of the card presents photographs of the holder's face, their name, date and place of birth (the latter in coded form), gender and marital status; the bottom quarter consists of machine-readable text. Three dates are listed as well; the date the citizen was first registered at RENIEC; the date the document was issued; and the expiration date of the document. The back of the DNI features the holder's address (including district, department and/or province) and voting group. Eight voting record blocks are successively covered with metallic labels when the citizen presents themselves at their voting group on voting days. The back also denotes whether the holder is an organ donor, presents the holder's right index finger print, a PDF417 bar code, and a 1D bar code.

Peruvian Documento Nacional de Identidad. (ISO ID-1)

Uruguay

Identity Card (Renewal)* [72]

In Uruguay, the identity card is issued by the Ministry of Interior and the National Civil Identification (DNIC). It is mandatory and essential for several steps at either governmental or private. The document is mandatory for all inhabitants of the Eastern Republic of Uruguay, are native citizens, legal citizens or resident aliens in the country, even for children from 45 days old.



Uruguayan Cédula de Identidad.

It is a laminated cardboard 9 cm wide and approximately 5 cm high, dominated by the blue color, showing the flag in the center of the Treinta y Tres Orientales, with the inscription "Liberty or Death." On the back appears the photo of the owner, the number assigned by the DNIC (Including a self-generated or check digit), name / s full / s with name / s and the corresponding signature (or proof of not knowing or not to sign). On the reverse appears nationality, date of birth, date of issuing the document and the date it is due (usually 10 years after the date of issue, even if issued after 70 years of age, lifetime and for the children is valid for five years). There is also the right thumbprint and observations if any.

Identity cards are demanded widespread in all formal transactions, from credit card purchases to any identity validation, proof of age, and so on.

Not to be confused with the civic badge, which is used exclusively for voting in elections (elections and plebiscites).

Check Digit Calculation ' They take the 7 card numbers and multiply each by 2987634 one by one (the first number by 2, the second by 9 and so on, when each result exceeds one digit, the unit takes only).

Example: UT: 1234567-X -> 2987634 -> 2, 8, 4, 8, 0, 8, 8

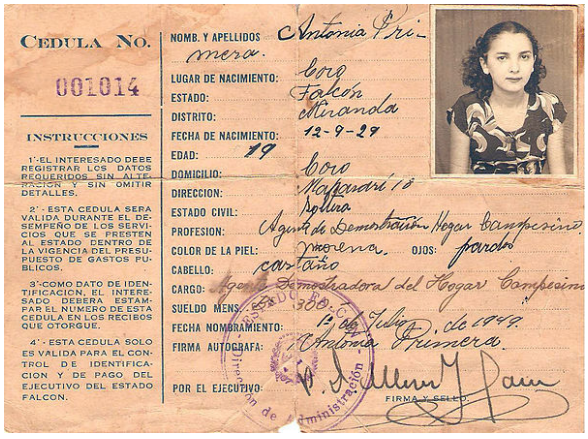
It is the sum of the results, the example would be 2 +8 +4 +8 +0 +8 +8 = 38 for the first number is greater than 38 that ends in 0 and is subtracted: 40-38 = 2 (is the same as 10 - (38 mod 10)). X = 2 then the check digit for the card 1,234,567.

Another simple way to look at it as a scalar product of vectors in module 10. The first 7 digits of the card can be viewed as a vector of length 7. This vector is multiplied by the vector scalar obtaining a number N 8123476 The check digit is found to be N module 10.

Example: CI: 1234567-X -> X = [(1x8) + (2x1) + (3x2) + (4x3) + (5x4) + (6x7) + (7x6)] mod 10 -> X = [8 +2 +6 +12 +20 +42 +42] mod 10 = 132 mod 10 = 2

Venezuela

Venezuelan Cédula de Identidad.



First class of bonds issued by the Government of Venezuela.

Identity cards in Venezuela consist of a plastic-laminated paper which contains the national ID number (*Cédula de Identidad*) as well as a color-photo and the last names, given names, date of birth, right thumb print, signature, and

marital status (single, married, divorced, widowed) of the bearer. It also contains the documents expedition and expiration date. Two different prefixes can be found before the ID number: "V" for Venezuelans and "E" for foreigners (*Extranjeros* in Spanish). This distinction is also shown in the document at the very bottom by a bold all-caps typeface displaying either the word VENEZOLANO or EXTRANJERO, respectively.

Despite Venezuela being the second country in the Americas (after the United States) to adopt a biometric passport, the current Venezuelan ID document is remarkably low-security, even for regional standards. It can hardly be called a card. The paper inside the laminated cover contains only two security measures, first, it is a special type of government-issued paper, and second, it has microfilaments in the paper that glow in the presence of UV light. The laminated cover itself is very simplistic and quite large for the paper it covers and the photo, although is standard sized (3x3.5 cm) is very blury. Government officials in charge of issuing the document openly recommend each individual to cut the excess plastic off and re-laminate the document in order to protect it from bending. The requirements for getting a Venezuelan identity document are quite relaxed and Venezuela lacks high-security in its birth certificates and other documents that give claim to citizenship.

Because one can get a Venezuelan passport and register to vote only by virtue of possessing a Venezuelan identity card, and since the Venezuelan government has been accused by the media and the opposition of naturalizing substantial amounts of foreigners for electoral purposes; many Venezuelans accused the government of a lack of a plan to ramp-up the security of the *cédula de identidad* along with other Venezuelan vital documents such as birth certificates as part of a strategy by the Chávez regime to continue the alleged practice of naturalizing foreigners for electoral purposes. The government has announced that a new *cédula de identidad* will be available to all citizens somewhere around the first quarter of 2011. This proposed ID is indeed a polycarbonate bankcard-sized document with biometric and RFID technology. It resembles the analogous card that has been in place in the Venezuelan biometric passports since 2007. However, the release of this new card to the public has been delayed in several occasions and as of March 2012 there are no news as to when it will be available.

11.4 See also

- List of identity card policies by country
- Access badge
- Anthropometry
- GlobalPlatform standard
- Home Return Permit
- ID card printer
- Location-based authentication
- Magnetic stripe card
- NO2ID
- Pass laws
- Physical security
- Police certificate
- Proximity card
- Warrant card

11.5 References

[1] "A brief history of the passport", The Guardian, 17 November 2006

[2] Ben Quarmby (2003-01-31). "The case for national identification cards". *2003 Duke L. & Tech. Rev. 0002*. Duke University. Retrieved 2008-01-11. If there is no reasonable expectation of privacy with regards to one's DNA information, the obtention of that information will not constitute a search. The DNA card scheme at issue here would not therefore come under 4th Amendment scrutiny

[3] "DNA ID Profiling and Banking". *Identigene website*. 2008-01-03. Archived from the original on 2007-10-27. Retrieved 2008-01-11. The powerful DNA profiling technology is encouraged to be used by parents when adopting newborn children. Insurance companies use DNA profiling as a precautionary tool to protect against life insurance fraud. Lawyers are bundling these services with packages, such as the Last Will and Testament, to assist in protecting the assets of large estates.

[4] "Surveillance & Identification: Identity". *Caslon Analytics research, analysis and strategies consultancy*. 2006-12-13. Retrieved 2008-01-11. As a German policeman once said, you are who your papers say you are. Take away those papers and you have no identity. Identification schemes - whether based on an individual's innate characteristics (e.g. DNA) or external attributes such as password or code number - facilitate participation by individuals with the requisite credentials in the "economic, social and political dimensions of society",

[5] "BEEsafe Personal ID program". Laboratory Collection Services. Archived from the original on 2007-12-14. Retrieved 2008-01-11. The area of the DNA molecule used for identification testing is known as a non-coding region.

This region gives absolutely no genetic information about your race, medical history, or pre-disposition to a disease. DNA is the ultimate tool for personal identification. Every individual has a unique set of DNA markers, which are inherited from their parents. Therefore, your loved one can be easily identified by their specific DNA profile. DNA Profiling is highly recommended by Law Enforcement Agencies nationwide as an identification method for all of your family. Acquiring a DNA Profile for your loved one is easy, painless, affordable, and need only be performed once, since his or her profile will not change over time.

[6] Garfinkel, Simson (January 2001) [2000]. "3 Absolute Identification" . *Database Nation: The Death of Privacy in the 21st Century* (Paperback). O'Reilly & Associates. ISBN 0-596-00105-3. When the technology was first introduced, scientists, lawyers, and civil libertarians argued over whether the underlying science was sound, and if the technology actually worked. Today, DNA identification is widely accepted as absolutely accurate--and we are struggling with the social implications of this newfound precision.

[7] Doward, Jamie (2005-05-29). "ID cards to cost £300 per person" . *The Guardian* (London). Retrieved 2010-05-05.

[8] "Cato Handbook, December 2004" (PDF). Retrieved 2012-07-01.

[9]

[10]

[11] "National Identity management Commission" . Nimc.gov.ng. Retrieved 2013-10-28.

[12] "Elections: FG okays INEC's national ID cards plan — The Punch - Nigeria's Most Widely Read Newspaper" . Punchng.com. 2013-04-11. Retrieved 2013-10-28.

[13] "SABC News.com - ID Smart Card launched in Union Buildings:Thursday 18 July 2013" . Sabc.co.za. 2013-07-18. Retrieved 2013-10-28.

[14] "Minister Naledi Pandor: Introduction of Smart Card Identity Document (Smart ID Cards) (English)". Info.gov.za. Retrieved 2013-10-28.

[15] "South Africa to pilot smart ID cards" .

[16] "A smart card that'll unite India - India News" . IBNLive. 2007-05-27. Retrieved 2012-07-01.

[17] Shenasnameh Laws and Services (Persian)

[18] Obligation of National ID number for Iranian citizens (Persian)

[19]

[20] Maan News - PA to remove religion from ID cards

[21] Al-Monitor - Hamas slams PA for removing religion from ID cards

[22] "Ministry of Internal Affairs and Communications | Local Administration Bureau(LAB)". Soumu.go.jp. Retrieved 2012-07-01.

[23] "MIC The Radio Use Website | Radio Operator System" . Tele.soumu.go.jp. 2011-03-31. Retrieved 2012-07-01.

[24] "Frequently Asked Questions" . Immigration Bureau of Japan. Retrieved 2013-10-27.

[25] "MSC Malaysia Flagship Applications" . Retrieved 28 December 2010.

[26] "One for All" . Retrieved 28 December 2010.

[27] "Identity Card services" . ICA. Retrieved 2012-07-01.

[28] "EU: UK Presidency advances EU-wide ID card standards, data retention and intelligence sharing to fight terrorism" . eGovernment News. 2005-07-14. Retrieved 2007-04-18.

[29] "Osobna iskaznica | AKD". Akd.hr. Retrieved 2013-10-28.

[30] idBlog - The number of electronic voters tripled

[31] Detailed results of Estonian European Parliament elections

[32] "Decree 55-1397 of October 22, 1955, initial version." (in French). Legifrance.gouv.fr. 1955-10-27. Retrieved 2012-07-01.

[33] "Decree 55-1397 of October 22, 1955" (in French). Legifrance.com. Retrieved 2012-07-01.

[34] "Code of criminal procedure, Book I, Title II, Chapter III" (in French). 195.83.177.9. Retrieved 2012-07-01.

[35] Service-Public.fr, Le site officiel de l'administration française. *Quelles sont les règles en matière de contrôle et de vérification d'identité ?*

[36] "Cass. crim. 05/02/2007, n°07-81517, Bull., n°112" (in French). Legifrance.gouv.fr. Retrieved 2012-07-01.

[37] "Cass. crim. 05/03/2007, n°07-81331, Bull., n°117" (in French). Legifrance.gouv.fr. Retrieved 2012-07-01.

[38] "Cass. crim. 05/12/1999, n°99-81153, Bull., n°95" (in French). Legifrance.gouv.fr. Retrieved 2012-07-01.

[39] http://www.kep.gov.gr/portal/page/portal/MyNewPortal?lng=us

[40] *Testo unico delle leggi di pubblica sicurezza* ("Single body of laws on public security"), also known as TULPS, article 3; see for example here .

[41] *Testo unico delle leggi di pubblica sicurezza* ("Single body of laws on public security"), also known as TULPS, article 157; see for example here .

[42] On lamination of ID cards, Web site of the municipality of Villa Cortese.

[43] "On identification of foreigners in Italy". Sicurezzapubblica.wikidot.com. Retrieved 2013-11-11.

[44] "Verificacion de Codigos DNI CIF NIF (validity check) NIE" (in Spanish). Argored s.l.

[45] Hernández Encinas, Luis; Espinosa García, Javier; Queiruga Dios, Araceli (September 2007). "The new Spanish electronic identity card: DNI-e". International Conference on Information Technologies (InfoTech-2007). vol I: Technological Aspects of the e-Governance and Data Protection. ISBN 978-954-9518-41-2. Retrieved 14 May 2011.

[46] "Spanish Identity Card BO-03001". European Council. 27 November 2009. Retrieved 15 May 2010.

[47] "Art 20.1 LOPSC".

[48] "Travel Documentation". Vueling. Retrieved 14 May 2014.

[49] "Frågor och svar om pass, nationellt id-kort och legitimation". Polisen.se. Retrieved 2012-07-01.

[50] "ID card database destroyed". Home Office. 2011-02-10. Retrieved 2012-07-01.

[51]

[52] "Godkjent legitimasjon". Nordea.no. Retrieved 2013-11-11.

[53] "Bankkortet skal ikke lenger være legitimasjon". Dinside.no. Retrieved 2013-11-11.

[54] Ble kastet av toget (Norwegian. Translation:Thrown off train)

[55] Serbian new biometric ID card (Serbian)

[56] Конзуларне земље - визе за иностранство

[57] EUobserver / Serbia and Kosovo sign first post-independence agreement

[58] Kosovo

[59] Ministria e Punëve të Jashtme

[60] "Junta Central Electoral de la República Dominicana - JCE > Dependencias > Cedulación > Tasas". JCE. Retrieved 2013-10-28.

[61] "¿Qué documentos se requieren para que los extranjeros obtengan su Cédula de Identidad ?". Soporte.jce.gob.do. Retrieved 2013-10-28.

[62] Curp gratis: Print your curp México

[63] "Intro". Student-ID.net. Retrieved March 12, 2014.

[64] Vijayan, Jaikumar (2008-12-22). "Obama will inherit a real mess on Real ID". Infoworld.com. Retrieved 2012-07-01.

[65] Rep. Thomas "Tom" Allen [D-ME1, 1997-2009]. "H.R. 1117: REAL ID Repeal and Identification Security Enhancement Act of 2007". Govtrack.us. Retrieved 2012-07-01.

[66] "Real Nightmare". Real Nightmare. Retrieved 2012-07-01.

[67] Driver's License or Passports Preferred ID at Checkpoints, retrieved May 30, 2008.

[68] "USCIS - USCIS Informs The Public That New Passport Card Is Acceptable For Employment Eligibility Verification". Uscis.gov. Retrieved 2012-07-01.

[69] "Passport Card". Germany.usembassy.gov. 2012-11-27. Retrieved 2013-11-11.

[70] "Home (Department of Transport and Main Roads)". Transport.qld.gov.au. 2012-06-19. Retrieved 2012-07-01.

[71] "Re.Na.Per - Ministerio del Interior – República Argentina". Nuevo DNI. Retrieved 2013-10-28.

[72] "Cédula de Identidad Renovación | Portal del Estado Uruguayo" (in Spanish). Tramites.gub.uy. 2012-03-23. Retrieved 2012-07-05.

11.6 Further reading

- Kruger, Stephen, "Documentary Identification in the Nascent American Police State" (2012). .
- Kruger, Stephen, "Police Demands for Hong Kong Identity Cards" (2012). .

11.7 External links

- HTTPS CARD - Internet identity card
- PRADO - Public Register of European Travel and ID Documents Online
- Telegraph story: the case for and against identity cards
- Scotsman story: ID Cards will lead to "massive fraud"
- ID Card – Is Big Brother Stalking You? –
- PRADO Glossary - EU site detailing document security technologies (security features)
- MP3 recording and reference list from Diffusion science radio program on 2SER broadcast on March 1, 2007.

Chapter 12

Alarm management

Alarm management is the application of human factors (or 'ergonomics') along with instrumentation engineering and systems thinking to manage the design of an alarm system to increase its usability. Most often the major usability problem is that there are too many alarms annunciated in a plant upset, commonly referred to as alarm flood (similar to an interrupt storm), since it is so similar to a flood caused by excessive rainfall input with a basically fixed drainage output capacity. However, there can also be other problems with an alarm system such as poorly designed alarms, improperly set alarm points, ineffective annunciation, unclear alarm messages, etc.

12.1 Alarm problem history

From their conception, large chemical, refining, power generation, and other processing plants required the use of a control system to keep the process operating successfully and producing products. Due to the fragility of the components as compared to the process, these control systems often required a control room to protect them from the elements and process conditions. In the early days of control rooms, they utilized what were referred to as "panel boards" which were loaded with control instruments and indicators. These were tied to sensors located in the process streams and on the outside of process equipment. The sensors relayed their information to the control instruments via analogue signals, such as a 4-20 mA current loop in the form of twisted pair wiring. At first these systems merely yielded information, and a well-trained operator was required to make adjustments either by changing flow rates, or altering energy inputs to keep the process within its designed limits.

Alarms were added to alert the operator to a condition that was about to exceed a design limit, or had already exceeded a design limit. Additionally, Emergency Shut Down (ESD) systems were employed to halt a process that was in danger of exceeding either safety, environmental or monetarily acceptable process limits. Alarm were indicated to the operator by annunciator horns, and lights of different colors. (For instance, green lights meant OK, Yellow meant not OK, and Red meant BAD.) Panel boards were usually laid out in a manner that replicated the process flow in the plant. So instrumentation indicating operating units with the plant was grouped together for recognition sake and ease of problem solution. It was a simple matter to look at the entire panel board, and discern whether any section of the plant was running poorly. This was due to both the design of the instruments and the implementation of the alarms associated with the instruments. Instrumentation companies put a lot of effort into the design and individual layout of the instruments they manufactured. To do this they employed behavioral psychology practices which revealed how much information a human being could collect in a quick glance. More complex plants had more complex panel boards, and therefore often more human operators or controllers.

Thus, in the early days of panel board systems, alarms were regulated by both real estate, and cost. In essence, they were limited by the amount of available board space, and the cost of running wiring, and hooking up an annunciator (horn), indicator (light) and switches to flip to acknowledge, and clear a resolved alarm. It was often the case that if you wanted a new alarm, you had to decide which old one to give up.

As technology developed, the control system and control methods were tasked to continue to advance a higher degree of plant automation with each passing year. Highly complex material processing called for highly complex control methodologies. Also, global competition pushed manufacturing operations to increase production while using less energy, and producing less waste. In the days of the panel boards, a special kind of engineer was required to understand a combination of the electronic equipment associated with process measurement and control, the control algorithms necessary to control the process (PID basics), and the actual process that was being utilized to make the products. Around the mid 80's, we entered the digital revolution. Distributed control systems (DCS) were a boon to the industry. The engineer could now control the process without having to understand the equipment necessary to per-

form the control functions. Panel boards were no longer required, because all of the information that once came across analog instruments could be digitized, stuffed into a computer and manipulated to achieve the same control actions once performed with amplifiers and potentiometers.

As a side effect, that also meant that alarms were easy and cheap to configure and deploy. You simply typed in a location, a value to alarm on and set it to active. The unintended result was that soon people alarmed everything. Initial installers set an alarm at 80% and 20% of the operating range of any variable just as a habit. One other unfortunate part of the digital revolution was that what once covered several square yards of real estate, now had to be fit into a 17 inch computer monitor. Multiple pages of information was thus employed to replicate the information on the replaced panel board. Alarms were utilized to tell an operator to go look at a page he was not viewing. Alarms were used to tell an operator that a tank was filling. Every mistake made in operations usually resulted in a new alarm. With the implementation of the OSHA 1910 regulations, HAZOPS studies usually requested several new alarms. Alarms were everywhere. Incidents began to accrue as a combination of too much data collided with too little useful information.

12.2 Alarm management history

Recognizing that alarms were becoming a problem, industrial control system users banded together and formed the Alarm Management Task Force, which was a customer advisory board led by Honeywell in 1990. The AMTF included participants from chemical, petrochemical, and refining operations. They gathered and wrote a document on the issues associated with alarm management. This group quickly realized that alarm problems were simply a subset of a larger problem, and formed the Abnormal Situation Management Consortium (ASM is a registered trademeark of Honeywell). The ASM Consortium developed a research proposal and was granted funding from the National Institute of Standards and Technology (NIST) in 1994. The focus of this work was addressing the complex human-system interaction and factors that influence successful performance for process operators. Automation solutions have often been developed without consideration of the human that needs to interact with the solution. In particular, alarms are intended to improve situation awareness for the control room operator, but a poorly configured alarm system does not achieve this goal.

The ASM Consortium has produced documents on best practices in alarm management, as well as operator situation awareness, operator effectiveness, and other operator-oriented issues. These documents were originally for ASM Consortium members only, but the ASMC has recently offered these documents publicly.[*] [1]

The ASM consortium also participated in development of an alarm management guideline published by the Engineering Equipment & Materials Users' Association (EEMUA) in the UK. The ASM Consortium provided data from their member companies, and contributed to the editing of the guideline. The result is EEMUA 191 “Alarm Systems- A Guide to Design, Management and Procurement” .

Several institutions and societies are producing standards on alarm management to assist their members in the best practices use of alarms in industrial manufacturing systems. Among them are the ISA (ISA SP-18), API (API 1167) and NAMUR (Namur NA 102). Several companies also offer software packages to assist users in dealing with alarm management issues. Among them are DCS manufacturing companies, and third-party vendors who offer add-on systems.

12.3 Concepts

The fundamental purpose of alarm annunciation is to alert the operator to deviations from normal operating conditions, i.e. abnormal operating situations. The ultimate objective is to prevent, or at least minimize, physical and economic loss through operator intervention in response to the condition that was alarmed. For most digital control system users, losses can result from situations that threaten environmental safety, personnel safety, equipment integrity, economy of operation, and product quality control as well as plant throughput. A key factor in operator response effectiveness is the speed and accuracy with which the operator can identify the alarms that require immediate action.

By default, the assignment of alarm trip points and alarm priorities constitute basic alarm management. Each individual alarm is designed to provide an alert when that process indication deviates from normal. The main problem with basic alarm management is that these features are static. The resultant alarm annunciation does not respond to changes in the mode of operation or the operating conditions.

When a major piece of process equipment like a charge pump, compressor, or fired heater shuts down, many alarms become unnecessary. These alarms are no longer independent exceptions from normal operation. They indicate, in that situation, secondary, non-critical effects and no longer provide the operator with important information. Similarly, during startup or shutdown of a process unit, many alarms are not meaningful. This is often the case because the static alarm conditions conflict with the required operating criteria for startup and shutdown.

In all cases of major equipment failure, startups, and shut-

downs, the operator must search alarm annunciation displays and analyze which alarms are significant. This wastes valuable time when the operator needs to make important operating decisions and take swift action. If the resultant flood of alarms becomes too great for the operator to comprehend, then the basic alarm management system has failed as a system that allows the operator to respond quickly and accurately to the alarms that require immediate action. In such cases, the operator has virtually no chance to minimize, let alone prevent, a significant loss.

In short, one needs to extend the objectives of alarm management beyond the basic level. It is not sufficient to utilize multiple priority levels because priority itself is often dynamic. Likewise, alarm disabling based on unit association or suppressing audible annunciation based on priority do not provide dynamic, selective alarm annunciation. The solution must be an alarm management system that can dynamically filter the process alarms based on the current plant operation and conditions so that only the currently significant alarms are annunciated.

The fundamental purpose of dynamic alarm annunciation is to alert the operator to relevant abnormal operating situations. They include situations that have a necessary or possible operator response to ensure:

- Personnel and Environmental Safety,
- Equipment Integrity,
- Product Quality Control.

The ultimate objectives are no different from the previous basic alarm annunciation management objectives. Dynamic alarm annunciation management focuses the operator's attention by eliminating extraneous alarms, providing better recognition of critical problems, and insuring swifter, more accurate operator response.*[2]

12.4 The need for alarm management

Alarm management is usually necessary in a process manufacturing environment that is controlled by an operator using a control system, such as a DCS or a programmable logic controller (PLC). Such a system may have hundreds of individual alarms that up until very recently have probably been designed with only limited consideration of other alarms in the system. Since humans can only do one thing at a time and can pay attention to a limited number of things at a time, there needs to be a way to ensure that alarms are presented at a rate that can be assimilated by a human operator, particularly when the plant is upset or in an unusual condition. Alarms also need to be capable of directing the operator's attention to the most important problem that he or she needs to act upon, using a priority to indicate degree of importance or rank, for instance.

12.5 Some improvement methods

The techniques for achieving rate reduction range from the extremely simple ones of reducing nuisance and low value alarms to redesigning the alarm system in a holistic way that considers the relationships among individual alarms.

12.5.1 Design guide

This step involves documenting the methodology or philosophy of how to design alarms. It can include things such as what to alarm, standards for alarm annunciation and text messages, how the operator will interact with the alarms.

12.5.2 Documentation and rationalization

This phase is a detailed review of all alarms to document their design purpose, and to ensure that they are selected and set properly and meet the design criteria. Ideally this stage will result in a reduction of alarms, but doesn't always.

12.5.3 Advanced methods

The above steps will often still fail to prevent an alarm flood in an operational upset, so advanced methods such as alarm suppression under certain circumstances are then necessary. As an example, shutting down a pump will always cause a low flow alarm on the pump outlet flow, so the low flow alarm may be suppressed if the pump was shut down since it adds no value for the operator, because he or she already knows it was caused by the pump being shut down. This technique can of course get very complicated and requires considerable care in design. In the above case for instance, it can be argued that the low flow alarm does add value as it confirms to the operator that the pump has indeed stopped.

Alarm management becomes more and more necessary as the complexity and size of manufacturing systems increases. A lot of the need for alarm management also arises because alarms can be configured on a DCS at nearly zero incremental cost, whereas in the past on physical control panel systems that consisted of individual pneumatic or electronic analog instruments, each alarm required expenditure and control panel real estate, so more thought usually went into the need for an alarm. Numerous disasters such as

Three Mile Island, Chernobyl accident and the Deepwater Horizon have established a clear need for alarm management.

12.6 The seven steps to alarm management*[3]

Step 1: Create and adopt an alarm philosophy

A comprehensive design and guideline document is produced which defines a plant standard employing a best-practise alarm management methodology.

Step 2: Alarm performance benchmarking

Analyze the alarm system to determine its strengths and deficiencies, and effectively map out a practical solution to improve it.

Step 3: "Bad actor"alarm resolution

From experience, it is known that around half of the entire alarm load usually comes from a relatively few alarms. The methods for making them work properly are documented, and can be applied with minimum effort and maximum performance improvement.

Step 4: Alarm documentation and rationalization (D&R)

A full overhaul of the alarm system to ensure that each alarm complies with the alarm philosophy and the principles of good alarm management.

Step 5: Alarm system audit and enforcement

DCS alarm systems are notoriously easy to change and generally lack proper security. Methods are needed to ensure that the alarm system does not drift from its rationalized state.

Step 6: Real-time alarm management

More advanced alarm management techniques are often needed to ensure that the alarm system properly supports, rather than hinders, the operator in all operating scenarios. These include Alarm Shelving, State-Based Alarming, and Alarm Flood Suppression technologies.

Step 7: Control and maintain alarm system performance

Proper management of change and longer term analysis and KPI monitoring are needed, to ensure that the gains that have been achieved from performing the steps above do not dwindle away over time. Otherwise they will; the principle of "entropy" definitely applies to an alarm system.

12.7 See also

- List of human-computer interaction topics, since most control systems are computer-based
- Design, especially interaction design
- Detection theory
- First-out alarm
- Physical security
- Annunciator panel

12.8 Notes

[1] ASM Consortium "Effective Alarm Management Guidelines".

[2] Jensen, Leslie D. "Dynamic Alarm Management on an Ethylene Plant". Retrieved 2008-05-22.

[3] Hollifield, Bill R. & Habibi, Eddie (2010). *The Alarm Management Handbook* (2 ed.). Houston, TX: PAS, Inc. pp. 35–182. ISBN 978-0-9778969-2-9.

12.9 References

- EPRI (2005) Advanced Control Room Alarm System: Requirements and Implementation Guidance. Palo Alto, CA. EPRI report 1010076.
- EEMUA 191 Alarm Systems - A Guide to Design, Management and Procurement (1999) ISBN 0-85931-076-0
- PAS - The Alarm Management Handbook - Second Edition (2010) ISBN 0-9778969-2-7
- SSM InfoTech Solutions Pvt. Ltd. - The Alarm Management Company Alarm Management System
- ASM Consortium (2009) - Effective Alarm Management Practices ISBN 978-1-4421-8425-1
- ANSI/ISA–18.2–2009 - Management of Alarm Systems for the Process Industries
- IEC 62682 Management of alarms systems for the process industries

12.10 External links

- "Principles for alarm system design" YA-711 Norwegian Petroleum Directorate

Chapter 13

Door security

Door security relates to prevention of door-related burglaries. Such break-ins take place in various forms, and in a number of locations; ranging from front, back and side doors to garage doors.

13.1 Common residential door types

The following are the types of doors typically used in residential applications: solid wood door, panel doors (hollow and solid core), metal skinned wood-edged doors and metal edge-wrapped doors. Typically, door frames are solid wood. Residential doors also frequently contain wood.

13.2 Security weakness of common residential door types

Security tests by *Consumer Reports Magazine* in the 1990s found that many residential doors fail or delaminate when force is applied to them. Solid wood doors withstood more force than the very common metal skinned wood-edged doors used in newer construction. A broad range door manufacturer, Premdor (now Masonite) once stated in one of its 1990s brochures entitled "Premdor Entry Systems" page 6 that "The results of tests were overwhelming, Steel edged doors outperform wood-edged doors by a ratio of 7 to 1. When you consider the practically two-thirds of all illegal entries were made through doors... One hit of 100 lb [lbf] strike force broke the wood-edged stile and opened the door. To actually open the steel-edged door required 7 strikes of 100 lb pressure [force]." Most door manufactures offer a number of different types of doors with varying levels of strength.

Consumer Reports Magazine also reported in its test results that door frames often split with little force applied and lower quality deadbolts simply failed when force was applied to the door.

The Chula Vista Residential Burglary Reduction Project which studied over 1,000 incidents found that "methods found to have relatively low effectiveness included: sliding glass door braces, such as wooden dowels, as opposed to sliding door channel or pin locks; deadbolts installed in the front door only; and outdoor lights on dusk-to-dawn timers". *[1]

13.3 Burglary tactics

The Chula Vista Residential Burglary-Reduction Project yielded the following findings: "From victim interviews, we learned that in 87% of the break-ins that occurred when intruders defeated locked doors with tools such as screwdrivers or crowbars, the burglars targeted "the one door that had no deadbolt lock ... not one burglar attempted to break a double-pane window during the course of successful or attempted burglary." *[1]

13.4 Door security devices

- **Alarms** —designed to warn of burglaries; this is often a silent alarm triggered when a door is opened while the alarm is active and the police or guards are warned without indication to the burglar, which increases the chances of catching him or her.

- **Burglar Deterrent CD or MP3s** —Home occupancy sounds recorded on a CD. The CD is played when the home owner is away, to mimic the home occupancy activities.

- **Deadbolts** —many manufacturers make deadbolts that are resistant to impact failure, picking and lock bumping. However, most deadbolts are not very secure.*[2] Consumer Reports Magazine's testing showed that many manufacturers make deadbolts that

break apart and otherwise fail when force is applied to the door.

- **Door strike reinforcers** —In general there are two products: frame reinforces, made to prevent delamination and or splitting of the door frame, and strike plate reinforcers, made to prevent the strike plate from being ripped out of the frame. Frame reinforces are metal strips installed vertically on or behind the door frame, on the hinge side they are known as Birmingham bars and on the strike plate side are known as London bars. Strike plate reinforcers secure the deadbolt pocket beyond the thin door frame material, directly to the stud or other wall.

- **Door reinforcements** —various products are made to prevent delamination and or splitting of the door. Sheet steel plate can be placed behind or under the deadbolt and wrap the door edge to prevent breaking the door around the deadbolt. Heavy duty products that place plates on either side the door tied together with screws or bolts can be used to prevent delamination.

- **Door chains** —allows the doors to be opened slightly to view outside while still remaining locked.

- **Secondary, internal locks** —sliding bolts, hooks and specialty latches, metal blocks or bars mounted internally.

- **Door viewers** —small fish-eye lenses that allow residents to view outside without opening the door.

- **Door windows** —there are three common methods to add security to windows in or beside doors: security bars and grates, security films (coatings applied to the glass in windows to reinforce it), or breakage resistant windows (plexiglas, lexan, and other glass replacement products).

- **Hinge screws** —longer or specialized screws that prevent the door from being simply pulled out after removing the hinge pins. Often the hinge pin itself is screwed, from the inside while to door is open, into the hinge to prevent removal of the hinge pin without first opening the door.

- **Sliding door / patio door locks** —there are numerous specialized products to prevent sliding doors from being defeated easily.

- **Visibility** —Most police departments recommend shrubs be cleared from near doorways to reduce the chance of a burglar being hidden from public view.

13.5 See also

- Access badge
- Access control
- Alarm management
- Biometrics
- Closed-circuit television
- Electronic lock
- ID Card
- Keycards
- Locksmithing
- Lock picking
- Magnetic stripe card
- Security lighting
- Surveillance

13.6 References

[1] The Chula Vista Residential Burglary Reduction Project - Summary

[2] Marc Weber Tobias - Locked, but not secure

Chapter 14

Guard tour patrol system

A **guard tour patrol system** is a system for logging the rounds of employees in a variety of situations such as security guards patrolling property, technicians monitoring climate-controlled environments, and correctional officers*[1] checking prisoner living areas. It helps ensure that the employee makes his or her appointed rounds at the correct intervals and can offer a record for legal or insurance reasons. Such systems have existed for many years using mechanical watchclock-based systems (watchman clocks/guard tour clocks/patrol clocks). Computerized systems were first introduced in Europe in the early 1980s, and in North America in 1986.*[2] Modern systems are based on handheld data loggers and RFID sensors.

The system provides a means to record the time when the employee reaches certain points on their tour. Checkpoints or watchstations are commonly placed at the extreme ends of the tour route and at critical points such as vaults, specimen refrigerators, vital equipment, and access points. Some systems are set so that the interval between stations is timed so if the employee fails to reach each point within a set time, other staff are dispatched to ensure the employee's well-being.

An example of a modern set-up might work as follows: The employee carries a portable electronic sensor (PES) or electronic data collector which is activated at each checkpoint. Checkpoints can consist of iButton semiconductors, magnetic strips, proximity microchips such as RFIDs, or optical barcodes. The data collector stores the serial number of the checkpoint with the date and time. Later, the information is downloaded from the collector into a computer where the checkpoint's serial number will have an assigned location (i.e. North Perimeter Fence, Cell Number 1, etc.). Data collectors can also be programmed to ignore duplicate checkpoint activations that occur sequentially or within a certain time period. Computer software used to compile the data from the collector can print out summaries that pinpoint missed checkpoints or patrols without the operator having to review all the data collected. Because devices can be subject to misuse, some have built-in microwave, g-force, and voltage detection.

In the analog age, the device used for this purpose was the watchclock.*[3] Watchclocks often had a paper or light cardboard disk placed inside for each 24-hour period. The user would carry the clock to each checkpoint, where a numbered key could be found (typically chained in place). The key would be inserted into the clock where it would imprint the disk. At the end of the shift or 24-hour period an authorized person (usually a supervisor) would unlock the watchclock and retrieve the disk.

14.1 Usages

Although this technology was initially developed for the security market, there are other uses. Some include:

- Public transport time table verification
- Hotel and hospital housekeeping logging
- Verification of patients being attended in hospitals by nursing staff
- Provide due diligence reports for retail slip & fall liability reduction
- Monitoring staff working outside of normal business hours

14.2 Criticisms

For routes which have significant outdoor exposure GPS units have proven to be an effective means of tracking security and law enforcement patrol behavior. GPS systems do not function in the most vulnerable areas such as indoors or underground. Accordingly, systems using assisted GPS have been developed.

14.3 References

[1] Paper on Law, Safety and Justice Capital Improvement Program, King County Washington, Page 6

[2] Clark, Bill; Robert R. Macdonald (March 1991). "High-Tech Touring". *Security Management* **35** (3): 25.

[3] The Detex Watchman's Clock Album, Philip Haselton. Accessed May 24, 2007.

Chapter 15

Security engineering

Security engineering is a specialized field of engineering that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts. It is similar to other systems engineering activities in that its primary motivation is to support the delivery of engineering solutions that satisfy pre-defined functional and user requirements, but with the added dimension of preventing misuse and malicious behavior. These constraints and restrictions are often asserted as a security policy.

In one form or another, security engineering has existed as an informal field of study for several centuries. For example, the fields of locksmithing and security printing have been around for many years.

Due to recent catastrophic events, most notably 9/11, Security Engineering has quickly become a rapidly growing field. In fact, in a recent report completed in 2006, it was estimated that the global security industry was valued at US$150 billion.*[1]

Security engineering involves aspects of social science, psychology (such as designing a system to 'fail well' instead of trying to eliminate all sources of error) and economics, as well as physics, chemistry, mathematics, architecture and landscaping.*[2] Some of the techniques used, such as fault tree analysis, are derived from safety engineering.

Other techniques such as cryptography were previously restricted to military applications. One of the pioneers of security engineering as a formal field of study is Ross Anderson.

15.1 Qualifications

Typical qualifications for a security engineer are:

- Professional Engineer, Chartered Engineer, Chartered Professional Engineer
- Certified Protection Professional (CPP) - International certification by ASIS International
- Physical Security Professional (PSP) - International certification by ASIS International
- Certified Information Systems Security Professional (CISSP)

However, multiple qualifications, or several qualified persons working together, may provide a more complete solution.*[3]

15.2 Security stance

The two possible default positions on security matters are:

1. **Default deny** - "Everything, not explicitly permitted, is forbidden"

   Improves security at a cost in functionality.

   This is a good approach if you have lots of security threats.

2. **Default permit** - "Everything, not explicitly forbidden, is permitted"

   Allows greater functionality by sacrificing security.

   This is only a good approach in an environment where security threats are non-existent or negligible.

   See computer insecurity for an example of the failure of this approach in the real world.

15.3 Core practices

- Security Requirements Analysis
- Secure coding
- Security testing
- Engineering Product Lifecycle
- Economics of security

15.4 Sub-fields

- Physical security
  - deter attackers from accessing a facility, resource, or information stored on physical media.
- Information security
  - protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption to access.
  - See esp. Computer security and Malice Engineering
- Technical surveillance counter-measures
- Economics of security
  - the economic aspects of economics of privacy and computer security.

15.5 Methodologies

Technological advances, principally in the field of computers, have now allowed the creation of far more complex systems, with new and complex security problems. Because modern systems cut across many areas of human endeavor, security engineers not only need consider the mathematical and physical properties of systems; they also need to consider attacks on the people who use and form parts of those systems using social engineering attacks. Secure systems have to resist not only technical attacks, but also coercion, fraud, and deception by confidence tricksters.

15.5.1 Web applications

According to the *Microsoft Developer Network* the patterns & practices of Security Engineering consists of the following activities:

- Security Objectives
- Security Design Guidelines
- Security Modeling
- Security Architecture and Design Review
- Security Code Review
- Security Testing
- Security Tuning
- Security Deployment Review

These activities are designed to help meet security objectives in the software life cycle.

15.5.2 Physical

Canadian Embassy in Washington, D.C. showing planters being used as vehicle barriers, and barriers and gates along the vehicle entrance

- Understanding of a *typical* threat and the usual risks to people and property.
- Understanding the incentives created both by the threat and the countermeasures.
- Understanding risk and threat analysis methodology and the benefits of an empirical study of the physical security of a facility.

- Understanding how to apply the methodology to buildings, critical infrastructure, ports, public transport and other facilities/compounds.
- Overview of common physical and technological methods of protection and understanding their roles in deterrence, detection and mitigation.
- Determining and prioritizing security needs and aligning them with the perceived threats and the available budget.

Target hardening

Whatever the target, there are multiple ways of preventing penetration by unwanted or unauthorised persons. Methods include placing Jersey barriers, stairs or other sturdy obstacles outside tall or politically sensitive buildings to prevent car and truck bombings. Improving the method of visitor management and some new electronic locks take advantage of technologies such as fingerprint scanning, iris or retinal scanning, and voiceprint identification to authenticate users.

15.6 Employers of security engineers

- US Department of State, Bureau of Diplomatic Security (ABET certified institution degree in engineering or physics required)*[4]
- Google*[5]
- Financial Services Industry, Health Care Industry,*[6] Energy Sector*[7]

15.7 Criticisms

15.7.1 Use of the term engineer

Main article: Controversies over the term Engineer

Some criticize this field as not being a bona fide field of engineering because the methodologies of this field are less formal or excessively ad-hoc compared to other fields and many in the practice of security engineering have no engineering degree.

15.8 See also

15.8.1 Further reading

- Ross Anderson (2001). *Security Engineering*. Wiley. ISBN 0-471-38922-6.
- Ross Anderson (2008). *Security Engineering - A Guide to Building Dependable Distributed Systems*. Wiley. ISBN 0-470-06852-3.
- Ross Anderson (2001). "Why Information Security is Hard - An Economic Perspective"
- Bruce Schneier (1995). *Applied Cryptography* (2nd edition ed.). Wiley. ISBN 0-471-11709-9.
- Bruce Schneier (2000). *Secrets and Lies: Digital Security in a Networked World*. Wiley. ISBN 0-471-25311-1.
- David A. Wheeler (2003). "Secure Programming for Linux and Unix HOWTO". *Linux Documentation Project*. Retrieved 2005-12-19.

15.8.2 Articles and papers

- patterns & practices Security Engineering on Channel9
- patterns & practices Security Engineering on MSDN
- patterns & practices Security Engineering Explained
- Basic Target Hardening from the Government of South Australia

15.9 References

[1] "Data analytics, networked video lead trends for 2008". *SP&T News* (CLB MEDIA INC). Retrieved 2008-01-05.

[2] "Landscaping for security". *Sunset*. 1988.

[3] http://www.asla.org/safespaces/pdf/design_brochure.pdf

[4] http://careers.state.gov/specialist/opportunities/seceng.html

[5] http://googleonlinesecurity.blogspot.com/2012/06/security-warnings-for-suspected-state.html

[6] "Senior Healthcare Security Engineer Jobs". Indeed.com. Retrieved 23 April 2014.

[7] "Network Security Engineer —Information Technology Jobs at Duke Energy Corporation". Jobs.com. Retrieved 23 April 2014.

Chapter 16

Surveillance

This article is about government surveillance. For the article about monitoring the spread of diseases, see disease surveillance. For other uses, see Surveillance (disambiguation).
"Electronic surveillance" redirects here. For surveillance of electronic computer systems, see Computer surveillance.

Surveillance (/sərˈveɪ.əns/ or /sərˈveɪləns/)[*][1] is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.[*][2] This can include observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls); and it can include simple, relatively no- or low-technology methods such as human intelligence agents and postal interception. The word *surveillance* comes from a French phrase for "watching over" ("sur" means "from above" and "veiller" means "to watch"), and is in contrast to more recent developments such as sousveillance.[*][3][*][4][*][5]

A 'nest' of surveillance cameras

Surveillance is used for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or for the investigation of crime. Surveillance can achieve this by three means: by deterrence, by observation and by reconstruction. Surveillance can deter by increasing the chance of being caught, and by revealing the modus operandi and accomplishes. This requires a minimal level of invasiveness.[*][6] Surveillance can detect by giving human operatives accurate and live situational awareness, and / or through the use of automated processes, i.e. video analytics. Surveillance can help reconstruct an incident through the availability of footage for forensics experts, perhaps again helped by video analytics. Surveillance can also influence subjective security if surveillance resources are visible or if the consequences of surveillance can be felt. In order to determine whether surveillance technology is actually improving surveillance, the effectiveness of surveillance must be expressed in terms of these higher purposes.

With the advent of programs such as the Total Information Awareness program and ADVISE, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance for Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of their subjects.[*][7] Many civil rights and privacy groups, such as the Electronic Frontier Foundation and American Civil Liberties Union, have expressed concern that by allowing continual increases in government surveillance of citizens we will end up in a mass surveillance society, with extremely limited, or non-existent political and/or personal freedoms. Fears such as this have led to numerous lawsuits such as *Hepting v. AT&T*.[*][7][*][8]

16.1 Types

16.1.1 Computer

Main article: Computer surveillance

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet.[*][9] In the

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

United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies.*[10]*[11]*[12]

There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups.*[13] Billions of dollars per year are spent, by agencies such as the Information Awareness Office, NSA, and the FBI, to develop, purchase, implement, and operate systems such as Carnivore, NarusInsight, and ECHELON to intercept and analyze all of this data, and extract only the information which is useful to law enforcement and intelligence agencies.*[14]

Computers can be a surveillance target because of the personal data stored on them. If someone is able to install software, such as the FBI's Magic Lantern and CIPAV, on a computer system, they can easily gain unauthorized access to this data. Such software could be installed physically or remotely.*[15] Another form of computer surveillance, known as van Eck phreaking, involves reading electromagnetic emanations from computing devices in order to extract data from them at distances of hundreds of meters.*[16]*[17] The NSA runs a database known as "Pinwale", which stores and indexes large numbers of emails of both American citizens and foreigners.*[18]*[19]

16.1.2 Telephones

Main article: Lawful interception

The official and unofficial tapping of telephone lines is widespread. In the United States for instance, the Communications Assistance For Law Enforcement Act (CALEA) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies.*[10]*[11]*[12] Two major telecommunications companies in the U.S.—AT&T Inc. and Verizon—have contracts with the FBI, requiring them to keep their phone call records easily searchable and accessible for Federal agencies, in return for $1.8 million per year.*[20] Between 2003 and 2005, the FBI sent out more than 140,000 "National Security Letters" ordering phone companies to hand over information about their customers' calling and Internet histories. About half of these letters requested information on U.S. citizens.*[21]

Human agents are not required to monitor most calls. Speech-to-text software creates machine-readable text from intercepted audio, which is then processed by automated call-analysis programs, such as those developed by agencies such as the Information Awareness Office, or companies such as Verint, and Narus, which search for certain words or phrases, to decide whether to dedicate a human agent to the call.*[22]

Law enforcement and intelligence services in the United Kingdom and the United States possess technology to activate the microphones in cell phones remotely, by accessing phones' diagnostic or maintenance features in order to listen to conversations that take place near the person who holds the phone.*[23]*[24]*[25]*[26]*[27]*[28]

Mobile phones are also commonly used to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily even when the phone is not being used, using a technique known as multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone.*[29]*[30] The legality of such techniques has been questioned in the United States, in particular whether a court warrant is required.*[31] Records for *one* carrier alone (Sprint), showed that in a given year federal law enforcement agencies requested customer location data 8 million times.*[32]

In response to customers' privacy concerns in the post Edward Snowden era, Apple's iPhone 6 has been designed to disrupt investigative wiretapping efforts. The phone en-

crypts e-mails, contacts, and photos with a code generated by a complex mathematical algorithm that is unique to an individual phone and is inaccessible to Apple.*[33] The encryption feature on the iPhone 6 has drawn criticism from FBI director James B. Comey and other law enforcement officials since even lawful requests to access user content on the iPhone 6 will result in Apple supplying "gibberish" data that requires law enforcement personnel to either break the code themselves or to get the code from the phone's owner.*[33] Because the Snowden leaks demonstrated that American agencies can access phones anywhere in the world, privacy concerns in countries with growing markets for smart phones have intensified, providing a strong incentive for companies like Apple to address those concerns in order to secure their position in the global market.*[33]

Although the CALEA requires telecommunication companies to build into their systems the ability to carry out a lawful wiretap, the law has not been updated to address the issue of smart phones and requests for access to e-mails and metadata.*[34] The Snowden leaks show that the NSA has been taking advantage of this ambiguity in the law by collecting metadata on "at least hundreds of millions" of "incidental" targets from around the world.*[34] The NSA uses an analytic tool known as CO-TRAVELLER in order to track people whose movements intersect and to find any hidden connections with persons of interest.*[34]

The Snowden leaks have also revealed that the British Government Communications Headquarters (GCHQ) can access information collected by the NSA on American citizens. Once the data has been collected, the GCHQ can hold on to it for up to two years. The deadline can be extended with the permission of a "senior UK official".*[35]

A surveillance camera in Cairns, Queensland

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

16.1.3 Cameras

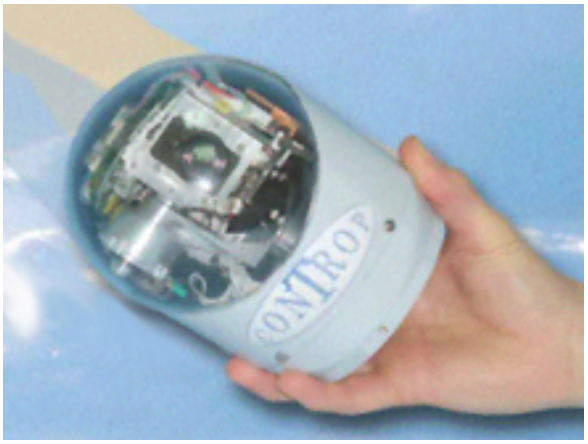
Main article: Closed-circuit television

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

In the United States, the Department of Homeland Security awards billions of dollars per year in Homeland Security grants for local, state, and federal agencies to install modern video surveillance equipment. For example, the city of Chicago, Illinois, recently used a $5.1 million Homeland Security grant to install an additional 250 surveillance cameras, and connect them to a centralized monitoring center, along with its preexisting network of over 2000 cameras, in a program known as Operation Virtual Shield. Speaking in 2009, Chicago Mayor Richard Daley announced that Chicago would have a surveillance camera on every street corner by the year 2016.*[36]*[37]

As part of China's Golden Shield Project, several U.S. corporations, including IBM, General Electric, and Honeywell, have been working closely with the Chinese government to install millions of surveillance cameras throughout China, along with advanced video analytics and facial recognition software, which will identify and track individuals every-

where they go. They will be connected to a centralized database and monitoring station, which will, upon completion of the project, contain a picture of the face of every person in China: over 1.3 billion people.*[38] Lin Jiang Huai, the head of China's "Information Security Technology" office (which is in charge of the project), credits the surveillance systems in the United States and the U.K. as the inspiration for what he is doing with the Golden Shield project.*[38]



A payload surveillance camera manufactured by Controp and distributed to the U.S. government by ADI Technologies

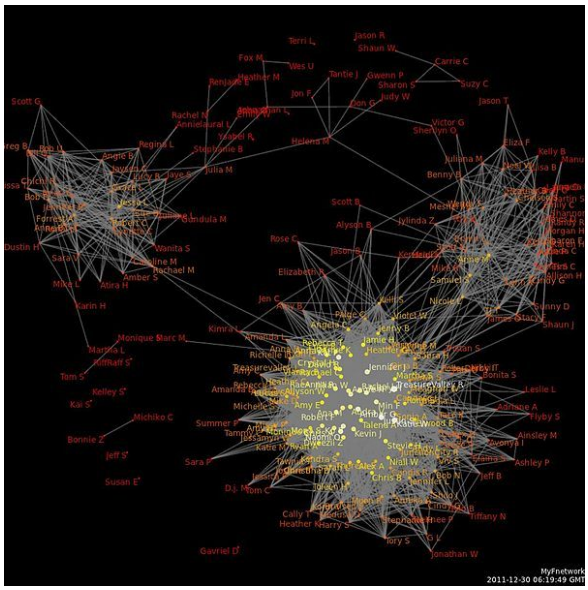
The Defense Advanced Research Projects Agency (DARPA) is funding a research project called Combat Zones That See that will link up cameras across a city to a centralized monitoring station, identify and track individuals and vehicles as they move through the city, and report "suspicious" activity (such as waving arms, looking side-to-side, standing in a group, etc.).*[39]

At Super Bowl XXXV in January 2001, police in Tampa, Florida, used Identix's facial recognition software, FaceIt, to scan the crowd for potential criminals and terrorists in attendance at the event *[40] (it found 19 people with pending arrest warrants).*[41]

Governments often initially claim that cameras are meant to be used for traffic control, but many of them end up using them for general surveillance. For example, Washington, D.C. had 5,000 "traffic" cameras installed under this premise, and then after they were all in place, networked them all together and then granted access to the Metropolitan Police Department, so they could perform "day-to-day monitoring".*[42]

The development of centralized networks of CCTV cameras watching public areas – linked to computer databases of people's pictures and identity (biometric data), able to track people's movements throughout the city, and identify whom they have been with – has been argued by some to present a risk to civil liberties.*[43] Trapwire is an example of such a network.*[44]

16.1.4 Social network analysis



A graph of the relationships between users on the social networking site Facebook. Social network analysis enables governments to gather detailed information about peoples' friends, family, and other contacts. Since much of this information is voluntarily made public by the users themselves, it is often consider to be a form of open-source intelligence

One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database,*[45] and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.*[46]*[47]*[48]*[49]

Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are investing heavily in research involving social network analysis.*[50]*[51] The intelligence community believes that the biggest threat to U.S. power comes from decentralized, leaderless, geographically dispersed groups of terrorists, subversives, extremists, and dissidents. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network.*[49]*[52]*[53]*[54]

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

> The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people.... In order to be successful SSNA will require information on the social interactions of the majority of people around the globe. Since the Defense Department cannot easily distinguish between peaceful citizens and terrorists, it will be necessary for them to gather data on innocent civilians as well as on potential terrorists.
> —Jason Ethier*[52]

AT&T developed a programming language called "Hancock", which is able to sift through enormous databases of phone call and Internet traffic records, such as the NSA call database, and extract "communities of interest"—groups of people who call each other regularly, or groups that regularly visit certain sites on the Internet. AT&T originally built the system to develop "marketing leads",*[55] but the FBI has regularly requested such information from phone companies such as AT&T without a warrant,*[55] and after using the data stores all information received in its own databases, regardless of whether or not the information was ever useful in an investigation.*[56]

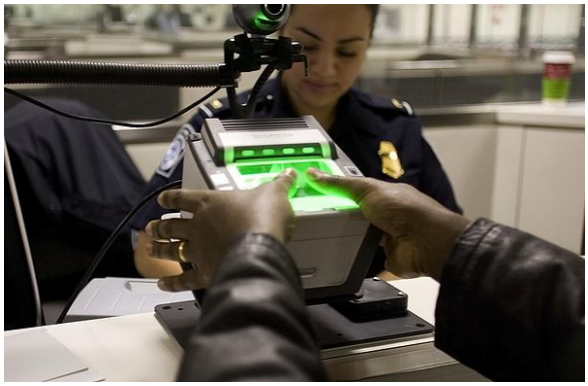
Some people believe that the use of social networking sites is a form of "participatory surveillance", where users of these sites are essentially performing surveillance on themselves, putting detailed personal information on public websites where it can be viewed by corporations and governments.*[46] In 2008, about 20% of employers reported using social networking sites to collect personal data on prospective or current employees.*[57]

16.1.5 Biometric

Main article: Biometrics

Biometric surveillance is any technology that measures and analyzes human physical and/or behavioral characteristics for authentication, identification, or screening purposes.*[58] Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioral characteristics include gait (a person's manner of walking) or voice.

Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video. Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems.*[59] The Information Processing Technology Office, ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft by their facial features.



Fingerprints being scanned as part of the US-VISIT program

Another form of behavioral biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioral traits. This might be used for instance to see if a person is acting "suspicious" (looking around furtively, "tense" or "angry" facial expressions, waving arms, etc.).*[60]

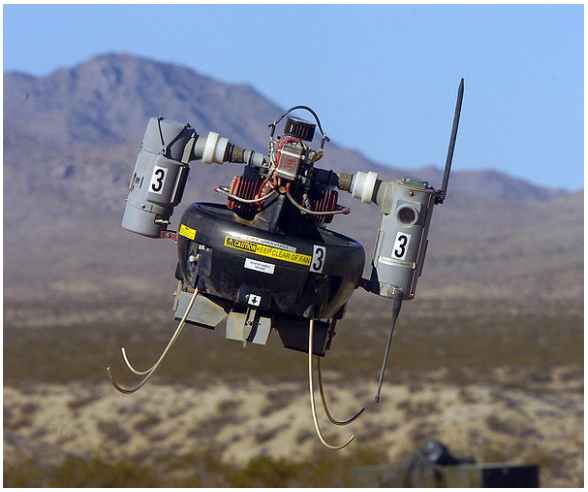
A more recent development is DNA fingerprinting, which looks at some of the major markers in the body's DNA to produce a match. The FBI is spending $1 billion to build a new biometric database, which will store DNA, facial recognition data, iris/retina (eye) data, fingerprints, palm prints, and other biometric data of people living in the United States. The computers running the database are contained in an underground facility about the size of two American football fields.*[61]*[62]*[63]

The Los Angeles Police Department is installing automated facial recognition and license plate recognition devices in its squad cars, and providing handheld face scanners, which officers will use to identify people while on patrol.*[64]*[65]*[66]

Facial thermographs are in development, which allow machines to identify certain emotions in people such as fear or stress, by measuring the temperature generated by blood flow to different parts of their face.*[67] Law enforcement officers believe that this has potential for them to identify when a suspect is nervous, which might indicate that they are hiding something, lying, or worried about some-

thing.*[67]

16.1.6 Aerial



Micro Air Vehicle with attached surveillance camera

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle—such as an unmanned aerial vehicle, helicopter, or spy plane. Military surveillance aircraft use a range of sensors (e.g. radar) to monitor the battlefield.

Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper,*[68] a U.S. drone plane used for domestic operations by the Department of Homeland Security, carries cameras that are capable of identifying an object the size of a milk carton from altitudes of 60,000 feet, and has forward-looking infrared devices that can detect the heat from a human body at distances of up to 60 kilometers.*[69] In an earlier instance of commercial aerial surveillance, the Killington Mountain ski resort hired 'eye in the sky' aerial photography of its competitors' parking lots to judge the success of its marketing initiatives as it developed starting in the 1950s.*[70]

The United States Department of Homeland Security is in the process of testing UAVs to patrol the skies over the United States for the purposes of critical infrastructure protection, border patrol, "transit monitoring", and general surveillance of the U.S. population.*[71] Miami-Dade police department ran tests with a vertical take-off and landing UAV from Honeywell, which is planned to be used in SWAT operations.*[72] Houston's police department has been testing fixed-wing UAVs for use in "traffic control".*[72]

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

The United Kingdom, as well, is working on plans to build up a fleet of surveillance UAVs ranging from micro-aerial vehicles to full-size drones, to be used by police forces throughout the U.K.*[73]

In addition to their surveillance capabilities, MAVs are capable of carrying tasers for "crowd control", or weapons for killing enemy combatants.*[74]

Programs such as the Heterogeneous Aerial Reconnaissance Team program developed by DARPA have automated much of the aerial surveillance process. They have developed systems consisting of large teams drone planes that pilot themselves, automatically decide who is "suspicious" and how to go about monitoring them, coordinate their activities with other drones nearby, and notify human operators if something suspicious is occurring. This greatly increases the amount of area that can be continuously monitored, while reducing the number of human operators required. Thus a swarm of automated, self-directing drones can automatically patrol a city and track suspicious individuals, reporting their activities back to a centralized monitoring station.*[75]*[76]*[77]

16.1.7 Data mining and profiling

Data mining is the application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data. Data profiling in this context is the process of assembling information about a particular individual or group in order to generate a profile —that is, a picture of their patterns and behavior. Data profiling can be an extremely powerful tool for psychological and social network analysis. A skilled analyst can discover facts about a person that they might not even be consciously aware of themselves.*[78]

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

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

Information relating to many of these individual transactions is often easily available because it is generally not guarded in isolation, since the information, such as the title of a movie a person has rented, might not seem sensitive. However, when many such transactions are aggregated they can be used to assemble a detailed profile revealing the actions, habits, beliefs, locations frequented, social connections, and preferences of the individual. This profile is then used, by programs such as ADVISE [*][79] and TALON, to determine whether the person is a military, criminal, or political threat.

In addition to its own aggregation and profiling tools, the government is able to access information from third parties —for example, banks, credit companies or employers, etc. —by requesting access informally, by compelling access through the use of subpoenas or other procedures,[*][80] or by purchasing data from commercial data aggregators or data brokers. The United States has spent $370 million on its 43 planned fusion centers, which are national network of surveillance centers that are located in over 30 states. The centers will collect and analyze vast amounts of data on U.S. citizens. It will get this data by consolidating personal information from sources such as state driver's licensing agencies, hospital records, criminal records, school records, credit bureaus, banks, etc. -- and placing this information in a centralized database that can be accessed from all of the centers, as well as other federal law enforcement and intelligence agencies.[*][81]

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

16.1.8 Corporate

Corporate surveillance is the monitoring of a person or group's behavior by a corporation. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. It can be used as a form of business intelligence, which enables the corporation to better tailor their products and/or services to be desirable by their customers. Or the data can be sold to other corporations, so that they can use it for the aforementioned purpose. Or it can be used for direct marketing purposes, such as the targeted advertisements on Google and Yahoo, where ads are targeted to the user of the search engine by analyzing their search history and emails[*][82] (if they use free webmail services), which is kept in a database.[*][83]

For instance, Google, the world's most popular search engine, stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months.[*][84] Google also scans the content of emails of users of its Gmail webmail service, in order to create targeted advertising based on what people are talking about in their personal email correspondences.[*][85] Google is, by far, the largest Internet advertising agency—millions of sites place Google's advertising banners and links on their websites, in order to earn money from visitors who click on the ads. Each page containing Google advertisements adds, reads, and modifies "cookies" on each visitor's computer.[*][86] These cookies track the user across all of these sites, and gather information about their web surfing habits, keeping track of which sites they visit, and what they do when they are on these sites. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use for building a profile of the user to deliver better-targeted advertising.[*][85]

According to the American Management Association and the ePolicy Institute that undertake an annual quantitative survey about electronic monitoring and surveillance with approximately 300 U.S. companies, "more than one fourth of employers have fired workers for misusing e-mail and nearly one third have fired employees for misusing the Internet".[*][87] More than 40% of the companies monitor e-mail traffic of their workers, and 66% of corporations monitor Internet connections. In addition, most companies use software to block non-work related websites such as sexual or pornographic sites, game sites, social networking sites, entertainment sites, shopping sites, and sport sites. The American Management Association and the ePolicy Institute also stress that companies "tracking content, keystrokes, and time spent at the keyboard ... store and review computer files ... monitor the blogosphere to see what is being written about the company, and ... monitor social networking sites

".[*][87] Furthermore, about 30% of the companies had also fired employees for non-work related email and Internet usage such as "inappropriate or offensive language "and" viewing, downloading, or uploading inappropriate/offensive content ".[*][87][*][88]

The United States government often gains access to these databases, either by producing a warrant for it, or by simply asking. The Department of Homeland Security has openly stated that it uses data collected from consumer credit and direct marketing agencies—such as Google—for augmenting the profiles of individuals whom it is monitoring.[*][83] The FBI, Department of Homeland Security, and other intelligence agencies have formed an "information-sharing" partnership with over 34,000 corporations as part of their Infragard program.

The U.S. Federal government has gathered information from grocery store "discount card" programs, which track customers' shopping patterns and store them in databases, in order to look for "terrorists" by analyzing shoppers' buying patterns.[*][89]

16.1.9 Human operatives

Organizations that have enemies who wish to gather information about the groups' members or activities face the issue of infiltration.[*][90][*][91]

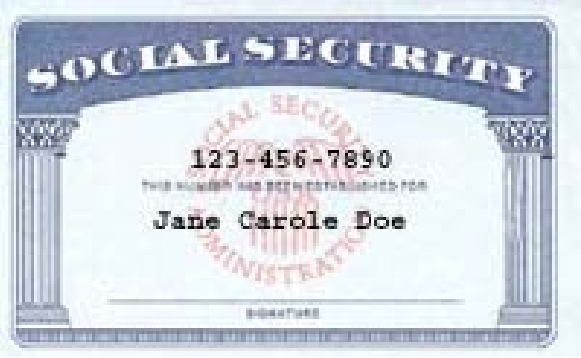
In addition to operatives' infiltrating an organization, the surveilling party may exert pressure on certain members of the target organization to act as informants (i.e., to disclose the information they hold on the organization and its members).[*][92][*][93]

Fielding operatives is very expensive, and for governments with wide-reaching electronic surveillance tools at their disposal the information recovered from operatives can often be obtained from less problematic forms of surveillance such as those mentioned above. Nevertheless, human infiltrators are still common today. For instance, in 2007 documents surfaced showing that the FBI was planning to field a total of 15,000 undercover agents and informants in response to an anti-terrorism directive sent out by George W. Bush in 2004 that ordered intelligence and law enforcement agencies to increase their HUMINT capabilities.[*][94]

16.1.10 Satellite imagery

On May 25, 2007 the U.S. Director of National Intelligence Michael McConnell authorized the National Applications Office (NAO) of the Department of Homeland Security to allow local, state, and domestic Federal agencies to access imagery from military intelligence satellites and aircraft sensors which can now be used to observe the activities of U.S. citizens. The satellites and aircraft sensors will be able to penetrate cloud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and will provide real-time video at much higher resolutions than the still-images produced by programs such as Google Earth.[*][95][*][96][*][97][*][98][*][99][*][100]

16.1.11 Identification and credentials



A card containing an identification number

One of the simplest forms of identification is the carrying of credentials. Some nations have an identity card system to aid identification, whilst others are considering it but face public opposition. Other documents, such as passports, driver's licenses, library cards, banking or credit cards are also used to verify identity.

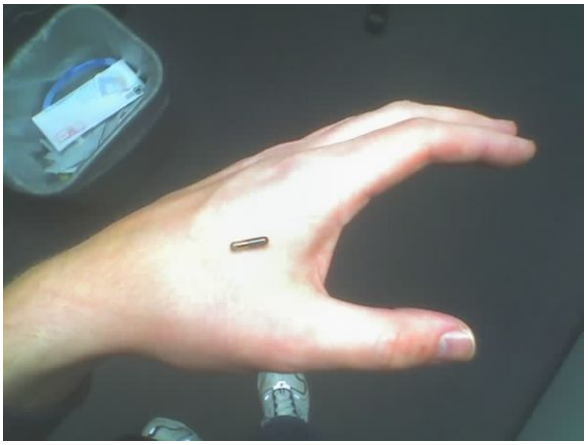
If the form of the identity card is "machine-readable", usually using an encoded magnetic stripe or identification number (such as a Social Security number), it corroborates the subject's identifying data. In this case it may create an electronic trail when it is checked and scanned, which can be used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

16.1.12 RFID and geolocation devices

RFID tagging

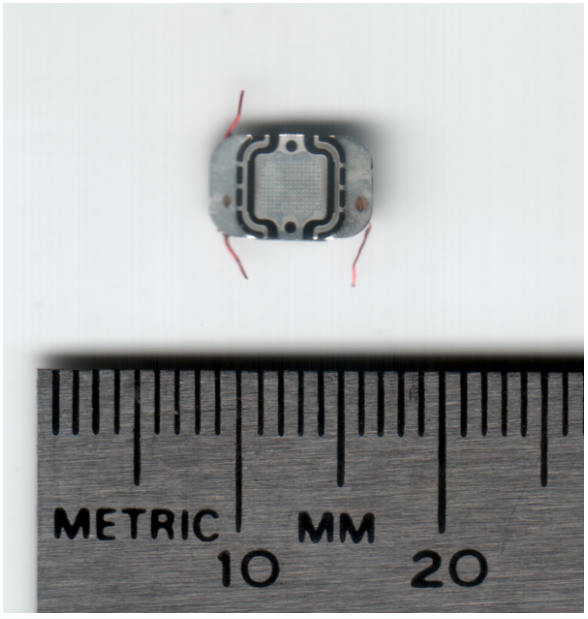
Radio Frequency Identification (RFID) tagging is the use of very small electronic devices (called "RFID tags") which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are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

Some companies appear to be "tagging" their workers by



Hand with planned insertion point for Verichip device

incorporating RFID tags in employee ID badges. Workers in U.K. considered strike action in protest of having themselves tagged; they felt that it was dehumanizing to have all of their movements tracked with RFID chips.*[101] Some critics have expressed fears that people will soon be tracked and scanned everywhere they go.*[102] On the other hand, RFID tags in newborn baby ID bracelets put on by hospitals have foiled kidnappings.*[101]



RFID chip pulled from new credit card

Verichip is an RFID device produced by a company called Applied Digital Solutions (ADS). Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc.'s database, the "Global VeriChip Subscriber Registry". Thousands of people have already had them inserted.*[102] In Mexico, for example, 160 workers at the Attorney General's office were required to have the chip injected for identity verification and access control purposes.*[103]*[104]

In a 2003 editorial, CNET News.com's chief political correspondent, Declan McCullagh, speculated that, soon, every object that is purchased, and perhaps ID cards, will have RFID devices in them, which would respond with information about people as they walk past scanners (what type of phone they have, what type of shoes they have on, which books they are carrying, what credit cards or membership cards they have, etc.). This information could be used for identification, tracking, or targeted marketing. As of 2012, this has largely not come to pass.*[105]

Global Positioning System

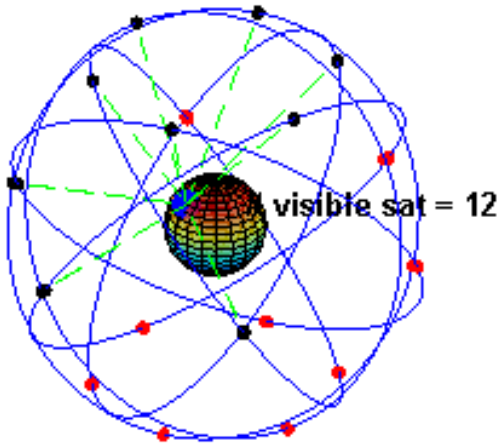


Diagram of GPS satellites orbiting Earth

See also: GPS tracking

In the U.S., police have planted hidden GPS tracking devices in people's vehicles to monitor their movements, without a warrant. In early 2009, they were arguing in court that they have the right to do this.*[106]

Several cities are running pilot projects to require parolees to wear GPS devices to track their movements when they get out of prison.*[107]

Mobile phones

Mobile phones are also commonly used to collect geolocation data. The geographical location of a mobile phone

(and thus the person carrying it) can be determined easily (whether it is being used or not), using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone.*[29]*[30]

Dr. Victor Kappeler*[108] of Eastern Kentucky University indicates that police surveillance is a strong concern, stating the following statistics from 2013:

> Of the 321,545 law enforcement requests made to Verizon, 54,200 of these requests were for "content" or "location" information—not just cell phone numbers or IP addresses. Content information included the actual text of messages, emails and the wiretapping of voice or messaging content in real-time.

16.1.13 Devices

See also: United States v. Spy Factory, Inc.

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

The U.S. has run numerous domestic intelligence, such as COINTELPRO, which have bugged the homes, offices, and vehicles of thousands of U.S. citizens, usually political activists, subversives, and criminals.*[109]

Law enforcement and intelligence services in the U.K. and the United States possess technology to remotely activate the microphones in cell phones, by accessing the phone's diagnostic/maintenance features, in order to listen to conversations that take place nearby the person who holds the phone.*[24]*[25]*[26]

16.1.14 Postal services

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

The U.S. Central Intelligence Agency and Federal Bureau of Investigation have performed twelve separate mail-opening campaigns targeted towards U.S. citizens. In one of these programs, more than 215,000 communications were intercepted, opened, and photographed.*[110]*[111]

16.2 Controversy

Graffiti expressing concern about proliferation of video surveillance

16.2.1 Support

Some supporters of surveillance systems believe that these tools protect society from terrorists and criminals. Other supporters simply believe that there is nothing that can be done about it, and that people must become accustomed to having no privacy. As Sun Microsystems CEO Scott McNealy said: "You have zero privacy anyway. Get over it."*[112]*[113]

Another common argument is: "If you aren't doing something wrong then you don't have anything to fear." Which follows that if one is engaging in unlawful activities, in which case they do not have a legitimate justification for their privacy. However, if they are following the law the surveillance would not affect them.*[114]

16.2.2 Opposition

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

An elaborate graffito in Columbus, Ohio, depicting state surveillance of telecommunications

privacy to watch over their own employee and secure their financial information it may become impossible, and they may not wish to hire those under surveillance. The most concern of detriment is securing the lives of those who live under total surveillance willingly, educating the public to those under peaceful watch while identifying terrorist and those who use the same surveillance systems and mechanisms in opposition to peace, against civilians, and to disclose lives removed from the laws of the land.

In addition, a significant risk of private data collection stems from the fact that this risk is too much unknown to be readily assessed today. Storage is cheap enough to have data stored forever, and the models using which it will be analyzed in a decade from now cannot reasonably be foreseen.*[115]

Totalitarianism

Programs such as the Total Information Awareness program, and laws such as the Communications Assistance For Law Enforcement Act have led many groups to fear that society is moving towards a state of mass surveillance with severely limited personal, social, political freedoms, where dissenting individuals or groups will be strategically removed in COINTELPRO-like purges.*[7]*[8]

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

Kate Martin, of the Center For National Security Studies said of the use of military spy satellites being used to monitor the activities of U.S. citizens: "They are laying the bricks one at a time for a police state." *[99]

Some point to the blurring of lines between public and private places, and the privatization of places traditionally seen as public (such as shopping malls and industrial parks) as illustrating the increasing legality of collecting personal information.*[116] Traveling through many public places such as government offices is hardly optional for most people, yet consumers have little choice but to submit to companies' surveillance practices.*[117] Surveillance techniques are not created equal; among the many biometric identification technologies, for instance, face recognition requires the least cooperation. Unlike automatic fingerprint reading, which requires an individual to press a finger against a machine, this technique is subtle and requires little to no consent.*[117]

Psychological/social effects

Some critics, such as Michel Foucault, believe that in addition to its obvious function of identifying and capturing individuals who are committing undesirable acts, surveillance also functions to create in everyone a feeling of always being watched, so that they become self-policing. This allows the State to control the populace without having to resort to physical force, which is expensive and otherwise problematic.*[118]

The concept of panopticism is a means of indirect control over a large populous through the uncertainty of surveillance. Michel Foucault analyzed the architecture of the prison panopticon, and realized that its success was not just in its ability to monitor but also its ability to not monitor without anyone knowing.*[119] Critics such as Derrick Jensen and George Draffan, argue that panopticism in the United States began in World War I when the issuing of passports became important for the tracking of citizens and possibly enemies of the state. Such surveillance continues today through government agencies in the form of tracking internet usage and library usage.*[120]

Psychologists have shown that merely giving people the "illusion" of being observed can produce significant voluntary changes in a range of pro-social behaviors.*[121] For example, studies have shown that people donate more and litter less when they think that they are being watched.

Privacy

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

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

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

16.3 Counter-surveillance, inverse surveillance, sousveillance

Countersurveillance is the practice of avoiding surveillance or making surveillance difficult. Developments in the late twentieth century have caused counter surveillance to dramatically grow in both scope and complexity, such as the Internet, increasing prevalence of electronic security systems, high-altitude (and possibly armed) UAVs, and large corporate and government computer databases.

Inverse surveillance is the practice of the reversal of surveillance on other individuals or groups (e.g., citizens photographing police). Well-known examples are George Holliday's recording of the Rodney King beating and the organization Copwatch, which attempts to monitor police officers to prevent police brutality. Counter-surveillance can be also used in applications to prevent corporate spying, or to track other criminals by certain criminal entities. It can also be used to deter stalking methods used by various entities and organizations.

Sousveillance is inverse surveillance, involving the recording by private individuals, rather than government or corporate entities.*[122]

16.4 Popular culture

16.4.1 In literature

- George Orwell's novel, *Nineteen Eighty-Four*, portrays a fictional totalitarian surveillance society with a very simple (by today's standards) mass surveillance system consisting of human operatives, informants, and two-way "telescreens" in people's homes. Because of the impact of this book, mass-surveillance technologies are commonly called "Orwellian" when they are considered problematic.
- The novel - *mistrust* highlights the negative effects from the overuse of surveillance at Reflection House. The central character *Kerryn* installs secret cameras to monitor her housemates - see also Paranoia
- The book *The Handmaid's Tale*, as well as a film based

on it, portray a totalitarian Christian theocracy where all citizens are kept under constant surveillance.

- In the book *The Girl with the Dragon Tattoo*, Lisbeth Salander uses computers to dig out information on people, as well as other common surveillance methods, as a freelancer.

16.4.2 In music

- The Dead Kennedys' song, "I Am The Owl", is about government surveillance and social engineering of political groups.

16.4.3 Onscreen

Main article: List of films featuring surveillance

- The movie, *Gattaca*, portrays a society that uses biometric surveillance to distinguish between people who are genetically engineered "superior" humans and genetically natural "inferior" humans.

- In the movie *Minority Report*, the police and government intelligence agencies use micro aerial vehicles in SWAT operations and for surveillance purposes.

- HBO's crime-drama series, *The Sopranos*, regularly portrays the FBI's surveillance of the DiMeo Crime Family. Audio devices they use include "bugs" placed in strategic locations (e.g., in "I Dream of Jeannie Cusamano" and "Mr. Ruggerio's Neighborhood") and hidden microphones worn by operatives (e.g., in "Rat Pack") and informants (e.g., in "Funhouse", "Proshai, Livushka" and "Members Only"). Visual devices include hidden still cameras (e.g., in "Pax Soprana") and video cameras (e.g., in "Long Term Parking").

- The movie, *THX-1138*, portrays a society wherein people are drugged with sedatives and antidepressants, and have surveillance cameras watching them everywhere they go.

- The movie, *The Lives of Others*, portrays the monitoring of East Berlin by agents of the Stasi, the GDR's secret police.

- The movie, *The Conversation*, portrays many methods of audio surveillance.

16.5 See also

- Big Brother Watch, a British civil liberties and privacy pressure group
- *Hepting v. AT&T*, a 2006 lawsuit by the Electronic Frontier Foundation (EFF) which alleges that AT&T assisted the National Security Agency (NSA) in unlawfully monitoring communications
- *Jewel v. NSA*, a lawsuit filed by the Electronic Frontier Foundation (EFF) against the National Security Agency (NSA) and several high-ranking U.S. government officials charging an "illegal and unconstitutional program of dragnet communications surveillance"
- Informational self-determination, a term for the capacity of the individual to determine in principle the disclosure and use of his/her personal data
- List of government surveillance projects
- Mass surveillance
  - Mass surveillance in Australia
  - Mass surveillance in China
  - Mass surveillance in East Germany
  - Mass surveillance in India
  - Mass surveillance in North Korea
  - Mass surveillance in the United Kingdom
  - Mass surveillance in the United States
- Panopticon, a type of institutional building designed to allow a watchman to observe (-opticon) all (pan-) inmates of an institution without their being able to tell whether they are being watched
- Privacy law
- Signals intelligence, intelligence-gathering by interception of communications and electronic signals
- Sousveillance (inverse surveillance), the recording of an activity by a participant in the activity
- Surveillance art, the use of surveillance technology to offer commentary on surveillance or surveillance technology
- Surveillance system monitor, a job that consists of monitoring closed circuit surveillance systems in order to detect crimes or disturbances
- Trapwire, a U.S. counter-terrorism technology company that produces software designed to find patterns indicative of terrorist attacks

16.5.1 United States government

- 2013 mass surveillance disclosures, reports about NSA and its international partners' mass surveillance of foreign nationals and U.S. citizens
- Bullrun (code name), a highly classified U.S. National Security Agency program to preserve its ability to eavesdrop on encrypted communications by influencing and weakening encryption standards, by obtaining master encryption keys, and by gaining access to data before or after it is encrypted either by agreement, by force of law, or by computer network exploitation (hacking)
- Carnivore, a U.S. Federal Bureau of Investigation system to monitor email and electronic communications
- COINTELPRO, a series of covert, and at times illegal, projects conducted by the FBI aimed at U.S. domestic political organizations
- Communications Assistance For Law Enforcement Act
- Computer and Internet Protocol Address Verifier (CIPAV), a data gathering tool used by the U.S. Federal Bureau of Investigation (FBI)
- Dropmire, a secret surveillance program by the NSA aimed at surveillance of foreign embassies and diplomatic staff, including those of NATO allies
- Heterogeneous Aerial Reconnaissance Team (HART), a DARPA project to develop systems for aerial surveillance of large urbanized areas using unmanned aerial vehicles
- Magic Lantern, keystroke logging software developed by the U.S. Federal Bureau of Investigation
- Mail Isolation Control and Tracking and Mail cover, programs to log metadata about all postal mail sent and received in the U.S.
- NSA call database, a database containing metadata for hundreds of billions of telephone calls made in the U.S.
- NSA warrantless surveillance (2001–07)
- NSA whistleblowers: William Binney, Thomas Andrews Drake, Mark Klein, Edward Snowden, Thomas Tamm, and Russ Tice
- Spying on United Nations leaders by United States diplomats
- Stellar Wind, code name for information collected under the President's Surveillance Program
- Terrorist Surveillance Program, an NSA electronic surveillance program
- Total Information Awareness, a project of the Defense Advanced Research Projects Agency (DARPA)

16.6 References

[1] OED

[2] Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.

[3] Minsky M, Kurzweil R, Mann S (2013). "The Society of Intelligent Veillance", Proceedings of the IEEE ISTAS 2013, Toronto, Ontario, Canada, pp13-17.

[4] Clarke, R. (1988). Information technology and dataveillance. Communications of the ACM, 31(5), 498-512.

[5] Michael, K., Roussos, G., Huang, G. Q., Gadh, R., Chattopadhyay, A., Prabhu, S., & Chu, P. (2010). Planetary-scale RFID services in an age of uberveillance. Proceedings of the IEEE, 98(9), 1663-1671.

[6] Deviant Behaviour - Socially accepted observation of behaviour for security, Jeroen van Rest

[7] "Is the U.S. Turning Into a Surveillance Society?". *American Civil Liberties Union*. Retrieved March 13, 2009.

[8] "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society". *American Civil Liberties Union*. January 15, 2003. Retrieved March 13, 2009.

[9] Diffie, Whitfield; Susan Landau (August 2008). "Internet Eavesdropping: A Brave New World of Wiretapping". *Scientific American*. Retrieved March 13, 2009.

[10] "CALEA Archive -- Electronic Frontier Foundation". *Electronic Frontier Foundation (website)*. Retrieved March 14, 2009.

[11] "CALEA: The Perils of Wiretapping the Internet". *Electronic Frontier Foundation (website)*. Retrieved March 14, 2009.

[12] "CALEA: Frequently Asked Questions". *Electronic Frontier Foundation (website)*. Retrieved March 14, 2009.

[13] Hill, Michael (October 11, 2004). "Government funds chat room surveillance research". USA Today. Associated Press. Retrieved March 19, 2009.

[14] McCullagh, Declan (January 30, 2007). "FBI turns to broad new wiretap method". *ZDNet News*. Retrieved September 26, 2014.

[15] "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats". Wired Magazine. July 18, 2007.

[16] Van Eck, Wim (1985). "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?". *Computers & Security* **4** (4): 269–286. doi:10.1016/0167-4048(85)90046-X.

[17] Kuhn, M.G. (2004). "Electromagnetic Eavesdropping Risks of Flat-Panel Displays". *4th Workshop on Privacy Enhancing Technologies*: 23–25.

[18] Risen, James; Lichtblau, Eric (June 16, 2009). "E-Mail Surveillance Renews Concerns in Congress". *New York Times*. pp. A1. Retrieved June 30, 2009.

[19] Ambinder, Marc (June 16, 2009). "Pinwale And The New NSA Revelations". *The Atlantic*. Retrieved June 30, 2009.

[20] Singel, Ryan (September 10, 2007). "Rogue FBI Letters Hint at Phone Companies' Own Data Mining Programs - Updated". *Threat Level* (Wired). Retrieved March 19, 2009.

[21] Roland, Neil (March 20, 2007). "Mueller Orders Audit of 56 FBI Offices for Secret Subpoenas". *Bloomberg News*. Retrieved March 19, 2009.

[22] Piller, Charles; Eric Lichtblau (July 29, 2002). "FBI Plans to Fight Terror With High-Tech Arsenal". *LA Times*. Retrieved March 14, 2009.

[23] Schneier, Bruce (December 5, 2006). "Remotely Eavesdropping on Cell Phone Microphones". *Schneier On Security*. Retrieved December 13, 2009.

[24] McCullagh, Declan; Anne Broache (December 1, 2006). "FBI taps cell phone mic as eavesdropping tool". *CNet News*. Retrieved March 14, 2009.

[25] Odell, Mark (August 1, 2005). "Use of mobile helped police keep tabs on suspect". *Financial Times*. Retrieved March 14, 2009.

[26] "Telephones". *Western Regional Security Office (NOAA official site)*. 2001. Retrieved March 22, 2009.

[27] "Can You Hear Me Now?". *ABC News: The Blotter*. Retrieved December 13, 2009.

[28] Coughlin, Kevin (December 13, 2006). "Even if they're off, cellphones allow FBI to listen in". *The Seattle Times*. Retrieved December 14, 2009.

[29] "Tracking a suspect by mobile phone". *BBC News*. August 3, 2005. Retrieved March 14, 2009.

[30] Miller, Joshua (March 14, 2009). "Cell Phone Tracking Can Locate Terrorists - But Only Where It's Legal". *FOX News*. Retrieved March 14, 2009.

[31] "Warrantless Location Tracking". *N.Y.U. Law Review*. 2008. Retrieved March 24, 2009.

[32] Zetter, Kim (December 1, 2009). "Threat Level Privacy, Crime and Security Online Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year". *Wired Magazine: Threat Level*. Retrieved December 5, 2009.

[33] Sanger, David (Sep 26, 2014). "Signaling Post-Snowden Era, New iPhone Locks Out N.S.A". *New York Times*. Retrieved November 1, 2014.

[34] Gellman, Barton (Dec 4, 2013). "NSA tracking cellphone locations worldwide, Snowden documents show". *The Washington Post*. Retrieved November 1, 2014.

[35] Nye, James (Oct 26, 2014). "British spies can go through Americans' telephone calls and emails without warrant revelas legal challenge in the UK". *Mail Online*. Retrieved November 1, 2014.

[36] Spielman, Fran (February 19, 2009). "Surveillance cams help fight crime, city says". *Chicago Sun Times*. Retrieved March 13, 2009.

[37] Schorn, Daniel (September 6, 2006). "We're Watching: How Chicago Authorities Keep An Eye On The City". *CBS News*. Retrieved March 13, 2009.

[38] Klein, Naomi (May 29, 2008). "China's All-Seeing Eye". *Rolling Stone*. Retrieved March 20, 2009.

[39] "Big Brother To See All, Everywhere". CBS News. Associated Press. July 1, 2003. Retrieved September 26, 2014.

[40] Bonsor, K. "How Facial Recognition Systems Work". Retrieved June 18, 2006.

[41] McNealy, Scott. "Privacy is (Virtually) Dead". Retrieved December 24, 2006.

[42] "Mayor Fenty Launches VIPS Program; New System Will Consolidate City's Closed-Circuit TV Monitoring". *www.dc.gov*. April 8, 2008. Retrieved March 13, 2009.

[43] "EPIC Video Surveillance Information Page". *EPIC*. Retrieved March 13, 2009.

[44] Hedgecock, Sarah (August 14, 2012). "TrapWire: The Less-Than-Advertised System To Spy On Americans". The Daily Beast. Retrieved 2012-09-13.

[45] Keefe, Patrick (March 12, 2006). ", Can Network Theory Thwart Terrorists?". *New York Times*.

[46] Albrechtslund, Anders (March 3, 2008). "Online Social Networking as Participatory Surveillance". *First Monday* **13** (3). Retrieved March 14, 2009.

[47] Fuchs, Christian (2009). *Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance*. Salzburg and Vienna: Forschungsgruppe Unified Theory of Information. ISBN 978-3-200-01428-2. Retrieved July 28, 2012.

[48] "Current Research in Social Network Theory". Retrieved 4 July 2014.

[49] "DyDAn Research Programs". *Homeland Security Center for Dynamic Data Analysis*. Retrieved December 20, 2009.

[50] Marks, Paul (June 9, 2006). "Pentagon sets its sights on social networking websites". *New Scientist*. Retrieved March 16, 2009.

[51] Kawamoto, Dawn (June 9, 2006). "Is the NSA reading your MySpace profile?". *CNET News*. Retrieved March 16, 2009.

[52] Ethier, Jason. "Current Research in Social Network Theory". *Northeastern University College of Computer and Information Science*. Retrieved March 15, 2009.

[53] Ressler, Steve (July 2006). "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research". *Homeland Security Affairs* **II** (2). Retrieved March 14, 2009.

[54] "DyDAn Research Blog". *DyDAn Research Blog (official blog of DyDAn)*. Retrieved December 20, 2009.

[55] Singel, Ryan (October 29, 2007). "AT&T Invents Programming Language for Mass Surveillance". *Threat Level* (Wired). Retrieved March 19, 2009.

[56] Singel, Ryan (October 16, 2007). "Legally Questionable FBI Requests for Calling Circle Info More Widespread than Previously Known". *Threat Level* (Wired). Retrieved March 19, 2009.

[57] Havenstein, Heather (September 12, 2008). "One in five employers uses social networks in hiring process". *Computer World*. Retrieved March 14, 2009.

[58] Woodward, John; Christopher Horn; Julius Gatune; Aryn Thomas (2003). *Biometrics: A Look at Facial Recognition*. RAND Corporation. ISBN 0-8330-3302-6. Retrieved March 15, 2009.

[59] Frank, Thomas (May 10, 2007). "Face recognition next in terror fight". *USA Today*. Retrieved March 16, 2009.

[60] Vlahos, James (January 2008). "Surveillance Society: New High-Tech Cameras Are Watching You". *Popular Mechanics*. Retrieved March 14, 2009.

[61] Nakashima, Ellen (December 22, 2007). "FBI Prepares Vast Database Of Biometrics: $1 Billion Project to Include Images of Irises and Faces". *Washington Post*. pp. A01. Retrieved May 6, 2009.

[62] Arena, Kelly; Carol Cratty (February 4, 2008). "FBI wants palm prints, eye scans, tattoo mapping". *CNN*. Retrieved March 14, 2009.

[63] Gross, Grant (February 13, 2008). "Lockheed wins $1 billion FBI biometric contract". *IDG News Service* (InfoWorld). Retrieved March 18, 2009.

[64] "LAPD: We Know That Mug". Wired Magazine. Associated Press. December 26, 2004. Retrieved March 18, 2009.

[65] Mack, Kelly. "LAPD Uses Face Recognition Technology To Fight Crime". *NBC4 TV (transcript from Officer.com)*. Retrieved December 20, 2009.

[66] Willon, Phil (September 17, 2009). "LAPD opens new high-tech crime analysis center". *LA Times*. Retrieved December 20, 2009.

[67] Dotinga, Randy (October 14, 2004). "Can't Hide Your Lying ... Face?". *Wired Magazine*. Retrieved March 18, 2009.

[68] Gasparre, Richard (January 25, 2008). "The U.S. and Unmanned Flight: Part 1". *airforce-technology.com*. Retrieved March 13, 2009.

[69] Fickes, Michael (October 1, 2004). "Automated Eye In The Sky". *GovernmentSecurity.com*. Retrieved March 13, 2009.

[70] Edwards, Bruce, "Killington co-founder Sargent dead at 83", Rutland *Herald*, November 9, 2012. Retrieved December 10, 2012.

[71] McCullagh, Declan (March 29, 2006). "Drone aircraft may prowl U.S. skies". *CNet News*. Retrieved March 14, 2009.

[72] Warwick, Graham (June 12, 2007). "US police experiment with Insitu, Honeywell UAVs". *FlightGlobal.com*. Retrieved March 13, 2009.

[73] La Franchi, Peter (July 17, 2007). "UK Home Office plans national police UAV fleet". *Flight International*. Retrieved March 13, 2009.

[74] "No Longer Science Fiction: Less Than Lethal & Directed Energy Weapons". *International Online Defense Magazine*. February 22, 2005. Retrieved March 15, 2009.

[75] "HART Overview". *IPTO (DARPA) -- Official website*. August 2008. Retrieved March 15, 2009.

[76] "BAA 04-05-PIP: Heterogeneous Airborne Reconnaissance Team (HART)". *Information Processing Technology Office (DARPA) -- Official Website*. December 5, 2003. Retrieved March 16, 2009.

[77] Sirak, Michael (Nov 29, 2007). "DARPA, Northrop Grumman Move Into Next Phase of UAV Control Architecture". *Defense Daily*. Retrieved March 16, 2009.

[78] Hildebrandt, Mireille; Serge Gutwirth (2008). *Profiling the European Citizen: Cross Disciplinary Perspectives*. Dordrecht: Springer. ISBN 978-1-4020-6913-0.

[79] Clayton, Mark (February 9, 2006). "US Plans Massive Data Sweep". *Christian Science Monitor*. Retrieved March 13, 2009.

[80] Flint, Lara (September 24, 2003). "Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power". *The Center For Democracy & Technology (official site)*. Retrieved March 20, 2009.

[81] ""National Network" of Fusion Centers Raises Specter of COINTELPRO". *EPIC Spotlight on Surveillance*. June 2007. Retrieved March 14, 2009.

[82] Story, Louise (November 1, 2007). "F.T.C. to Review Online Ads and Privacy". *New York Times*. Retrieved March 17, 2009.

[83] Butler, Don (February 24, 2009). "Surveillance in society". *The Star Phoenix* (CanWest). Retrieved March 17, 2009.

[84] Soghoian, Chris (September 11, 2008). "Debunking Google's log anonymization propaganda". *CNET News*. Retrieved March 21, 2009.

[85] Joshi, Priyanki (March 21, 2009). "Every move you make, Google will be watching you". *Business Standard*. Retrieved March 21, 2009.

[86] "Advertising and Privacy". *Google (company page)*. 2009. Retrieved March 21, 2009.

[87] American Management Association and the ePolicy Institute (2008). Electronic Monitoring and Surveillance 2007 Survey. Retrieved July 27, 2012.

[88] Allmer, Thomas (2012). Towards a Critical Theory of Surveillance in Informational Capitalism. Frankfurt am Main: Peter Lang.

[89] Vlahos, Kelley (August 1, 2002). "Store Customer Cards a Source for FBI?". *FOX News*. Retrieved March 17, 2009.

[90] anonymous (Jan 26, 2006). "Information on the Confidential Source in the Auburn Arrests". *Portland Indymedia*. Retrieved March 13, 2009.

[91] Myers, Lisa (December 14, 2005). "Is the Pentagon spying on Americans?". *NBC Nightly News* (msnbc.com). Retrieved March 13, 2009.

[92] "Senate Hearing: The Use Of Informants In FBI Domestic Intelligence Investigations". *SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS*. U.S. Senate. April 23, 1976. Retrieved March 13, 2009.

[93] Ranalli, Ralph (November 21, 2003). "FBI informant system called a failure". *Boston Globe*. Retrieved March 13, 2009.

[94] Ross, Brian (July 25, 2007). "FBI Proposes Building Network of U.S. Informants". *Blotter*. ABC News. Retrieved March 13, 2009.

[95] "U.S. Reconnaissance Satellites: Domestic Targets". *National Security Archive*. Retrieved March 16, 2009.

[96] Block, Robert (August 15, 2007). "U.S. to Expand Domestic Use Of Spy Satellites". *Wall Street Journal*. Retrieved March 14, 2009.

[97] Gorman, Siobhan (October 1, 2008). "Satellite-Surveillance Program to Begin Despite Privacy Concerns". *The Wall Street Journal*. Retrieved March 16, 2009.

[98] "Fact Sheet: National Applications Office". *Department of Homeland Security (official website)*. August 15, 2007. Retrieved March 16, 2009.

[99] Warrick, Joby (August 16, 2007). "Domestic Use of Spy Satellites To Widen". *Washington Post*. pp. A01. Retrieved March 17, 2009.

[100] Shrader, Katherine (September 26, 2004). "Spy imagery agency watching inside U.S.". USA Today. Associated Press. Retrieved March 17, 2009.

[101] "Two Stories Highlight the RFID Debate". *RFID Journal*. July 19, 2005. Retrieved March 23, 2012.

[102] Lewan, Todd (July 21, 2007). "Microchips in humans spark privacy debate". USA Today. Associated Press. Retrieved March 17, 2009.

[103] Gardener, W. David (July 15, 2004). "RFID Chips Implanted In Mexican Law-Enforcement Workers". *Information Week*. Retrieved March 17, 2009.

[104] Campbell, Monica (August 4, 2004). "Law enforcement in Mexico goes a bit bionic". *Christian Science Monitor*. Retrieved March 17, 2009.

[105] McCullagh, Declan (January 13, 2003). "RFID Tags: Big Brother in small packages". *CNET News*. Retrieved July 24, 2012.

[106] Claburn, Thomas (March 4, 2009). "Court Asked To Disallow Warrantless GPS Tracking". *Information Week*. Retrieved March 18, 2009.

[107] Hilden, Julie (April 16, 2002). "What legal questions are the new chip implants for humans likely to raise?". *CNN.com (FindLaw)*. Retrieved March 17, 2009.

[108] Kappeler, Victor. "Forget the NSA: Police May be a Greater Threat to Privacy".

[109] Wolf, Paul. "COINTELPRO". *(online collection of historical documents)*. Retrieved March 14, 2009.

[110] "SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: ... DOMESTIC CIA AND FBI MAIL OPENING PROGRAMS". *SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES UNITED STATES SENATE*. April 23, 1976. Retrieved March 13, 2009.

[111] Goldstein, Robert. *Political Repression in Modern America*. University of Illinois Press. ISBN 978-0-252-06964-2.

[112] Sprenger, Polly (January 26, 1999). "Sun on Privacy: 'Get Over It'". *Wired Magazine*. Retrieved March 20, 2009.

[113] Baig, Edward; Marcia Stepanek; Neil Gross (April 5, 1999). "Privacy". *Business Week*. Retrieved March 20, 2009.

[114] Solove, Daniel (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". *San Diego Law Review* **44**: 745.

[115] "Against the collection of private data: The unknown risk factor". March 8, 2012.

[116] Marx, G. T., & Muschert, G. W. (2007). Personal information, borders, and the new surveillance studies. Annual Review of Law and Social Science, 3, 375-395.

[117] Agre, P. (2003). Your Face is not a bar code: arguments against automatic face recognition in public places. Retrieved November 14, 2004, from http://polaris.gseis.ucla.edu/pagre/bar-code.html

[118] Foucault, Michel (1979). *Discipline and Punish*. New York: Vintage Books. pp. 201–202.

[119] Foucault, Michel (1995). *Discipline and Punish*. New York: Random House. pp. 200–203.

[120] Jensen, Derrick (2004). , *Welcome to the Machine: Science, Surveillance and the Culture of Control*. Vermont: Chelsea Green Publishing. pp. 112–124.

[121] van der Linden, Sander (March 2011). "How the Illusion of Being Observed can Make You a Better Person". *Scientific American*. Retrieved September 10, 2014.

[122] Birch, Dave (July 14, 2005). "The age of sousveillance". *The Guardian* (London). Retrieved August 6, 2007.

16.7 Further reading

- Garfinkel, Simson, *Database Nation; The Death of Privacy in the 21st Century*. O'Reilly & Associates, Inc. ISBN 0-596-00105-3
- Gilliom, John *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*, University Of Chicago Press, ISBN 978-0-226-29361-5
- Jenkins, Peter *Advanced Surveillance Training Manual*, Intel Publishing, UK ISBN 0-9535378-1-1
- Jensen, Derrick and Draffan, George (2004) *Welcome to the Machine: Science, Surveillance, and the Culture of Control* Chelsea Green Publishing Company. ISBN 978-1-931498-52-4
- Lyon, David (2001). *Surveillance Society: Monitoring in Everyday Life*. Philadelphia: Open University Press. ISBN 978-0-335-20546-2
- Lyon, David (2007) *Surveillance Studies: An Overview*. Cambridge: Polity Press. ISBN 978-0-7456-3591-0
- Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, eds. (2012). "Internet and Surveillance: The Challenges of Web 2.0 and Social Media". New York: Routledge. ISBN 978-0-415-89160-8
- Parenti, Christian *The Soft Cage: Surveillance in America From Slavery to the War on Terror*, Basic Books, ISBN 978-0-465-05485-5
- Harris, Shane. (2011). *The Watchers: The Rise of America's Surveillance State*. London, UK: Penguin Books Ltd. ISBN 0-14-311890-0
- Matteralt, Armand. (2010). *The Globalization of Surveillance*. Cambridge, UK: Polity Press. ISBN 0-7456-4511-9
- Feldman, Jay. (2011). *Manufacturing Hysteria: A History of Scapegoating, Surveillance, and Secrecy in Modern America*. New York, NY: Pantheon Books. ISBN 0-375-42534-9
- Hier, Sean P., & Greenberg, Joshua (Eds.). (2009). *Surveillance: Power, Problems, and Politics*. Vancouver, CA: UBC Press. ISBN 0-7748-1611-2
- Lyon, David (Ed.). (2006). *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, UK: Willan Publishing. ISBN 978-1-84392-191-2
- Laidler, Keith. (2008). *Surveillance Unlimited: How We've Become the Most Watched People on Earth*. Cambridge, AU: Icon Books Ltd. ISBN 978-1-84046-877-9
- Staples, William G. (2000). *Everyday Surveillance: Vigilance and Visibility in Post-Modern Life*. Lanham, MD: Rowman & Littlefield Publishers. ISBN 0-7425-0077-2
- Allmer, Thomas (2012). "Towards a Critical Theory of Surveillance in Informational Capitalism". Frankfurt am Main: Peter Lang. ISBN 978-3-631-63220-8

16.8 External links

16.8.1 General information

- ACLU, "The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society"

- Balkin, Jack M. (2008). "The Constitution in the National Surveillance State", Yale Law School
- Bibo, Didier and Delmas-Marty, "The State and Surveillance: Fear and Control"
- EFF Privacy Resources
- EPIC Privacy Resources
- ICO. (September 2006). "A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network".
- Privacy Information Center
- "The NSA Files (Dozens of articles about the U.S. National Security Agency and its spying and surveillance programs)". *The Guardian* (London). June 8, 2013.
- "Special Issue on Surveillance Capitalism - nine articles analyzing economic, financial, social, political, legal, security and other aspects of US and international surveillance and spying programs and their relation to capitalism". *Monthly Review*. August 2014. (Volume 66, Number 3)

16.8.2 Historical information

- COINTELPRO —FBI counterintelligence programs designed to neutralize political dissidents
- Reversing the Whispering Gallery of Dionysius - A Short History of Electronic Surveillance in the United States

16.8.3 Legal resources

- EFF Legal Cases
- Guide to lawful intercept legislation around the world

16.9 Text and image sources, contributors, and licenses

16.9.1 Text

- **Security** *Source:* http://en.wikipedia.org/wiki/Security?oldid=636790628 *Contributors:* WojPob, The Anome, Koyaanis Qatsi, Enchanter, Heron, Hephaestos, Edward, Patrick, Michael Hardy, Kku, Mic, Dori, Pagingmrherman, Ahoerstemeier, Ronz, BigFatBuddha, Julesd, Andrewman327, WhisperToMe, DJ Clayworth, Tempshill, Chrisbrown, Joy, Mackensen, Cncs wikipedia, Robbot, ChrisO, Moriori, Jmabel, Steeev, Roscoe x, Pengo, DocWatson42, MathKnight, Revth, Brockert, Tinidril, Antandrus, Quarl, Mozzerati, Karl-Henner, Brianjd, Jpg, Cacycle, ArnoldReinhold, Aranel, RoyBoy, Causa sui, JRM, Smalljim, Matt Britt, Maurreen, Minghong, Pearle, Poli, Storm Rider, Alansohn, M7, Kurieeto, Suruena, HenkvD, Docboat, H2g2bob, BlastOButter42, Drbreznjev, Woohookitty, Uncle G, Commander Keane, Bennetto, Davidfstr, Eras-mus, Gerbrant, Sinar, Fcoulter, Wikix, DeadlyAssassin, MZMcBride, Vegaswikian, Bhadani, SNIyer12, CCRoxtar, FlaBot, Old Moonraker, Gurch, Common Man, Imnotminkus, Coolhawks88, DVdm, Dzzl, VolatileChemical, Abby724, UkPaolo, Sceptre, Muchness, Backburner001, Peter S., Stephenb, Cryptic, Draeco, Wiki alf, Grafen, AlMac, Irishguy, Nick, Toddgee, Wsiegmund, Exit2DOS2000, Luk, DocendoDiscimus, Veinor, SmackBot, Reedy, Ominae, Londonlinks, Ohnoitsjamie, Kazkaskazkasako, Oli Filth, ERobson, Kungming2, Jmax-, Dethme0w, Frap, CelebritySecurity, Yidisheryid, COMPFUNK2, Derek R Bullamore, Weregerbil, DMacks, Rory096, Kuru, JHunterJ, Stupid Corn, Beetstra, Jadams76, Yaxh, Jose77, Ice-Evil, Levineps, Iridescent, Astharoth1, Shoeofdeath, Sander Säde, Courcelles, SkyWalker, Wafulz, Andrewia, Iceturf, AshLin, HerveB, ShelfSkewed, Nnp, Mapletip, Gogo Dodo, ST47, Biblbroks, Maziotis, Spineofgod, Mojo Hand, Mentifisto, AntiVandalBot, Luna Santin, Dbrodbeck, Marokwitz, Prolog, MER-C, Tqbf, SiobhanHansa, Magioladitis, VoABot II, JamesBWatson, JohnLai, Havanafreestone, JaGa, Klf uk, Jim.henderson, Uvainio, Kostisl, R'n'B, CommonsDelinker, J.delanoy, Dbiel, WarthogDemon, Reedy Bot, Touch Of Light, Shoman93, JHeinonen, BigHairRef, Idioma-bot, Technowonk, Jeff G., TheMindsEye, Bsroiaadn, Touchingwater, Philip Trueman, Mercy, Perohanych, HansWDaniel, Qxz, Meters, Altermike, Kbrose, K. Annoyomous, Bob Costello, Moonriddengirl, Derekcslater, Caltas, Lucca.Ghidoni, Oda Mari, Oxymoron83, Corp Vision, Spitfire19, Correogsk, Disooqi, Hariva, Pinkadelica, Martarius, ClueBot, The Thing That Should Not Be, Ark2120, Drmies, Sushilover boy, Nesberries, Lartoven, Heyta, SchreiberBike, DanielPharos, Aitias, PCHS-NJROTC, Portal60hooch, XLinkBot, Timschocker, Rror, SilvonenBot, Loganmstarr, Exegete48, Lakerfan48, Addbot, Adamylo, WeatherFug, TutterMouse, Fieldday-sunday, MrOllie, Latiligence, DreamHaze, OffsBlink, Tide rolls, Luckas Blade, Exegetetheology, PlankBot, Electronicommerce, Yobot, Fraggle81, Andyj00, Onyx020, Kcmoduk, Angel ivanov angelov, Orion11M87, AnomieBOT, Andrewrp, Galoubet, Jungle-Jym2, ChristopheS, Materialscientist, GB fan, Neurolysis, Mlduda, Bihco, Mysecurecyberspace, Zoom-Arrow, EFE YILDIRIM, Alvin Seville, Tulocci, Joxemai, Voltov45, Jakejo2009, Track1200, Spasioc, Untchable, Isecom, Laaa200, Oczwap, Burrettwilce, SpaceFlight89, Mentmic, Meaghan, Supergreg no1, Reconsider the static, Jonkerz, Lotje, Stopspam4567, Maxlaker, Ragle Fragle 007, Wanne673, Reach Out to the Truth, T0jikist0ni, Deagle AP, Nothingmore Nevermore, We hope, Redeyeglasses, 2beornot57, Greatread, Netknowle, Staszek Lem, Bosnabosna, L Kensington, Sepersann, RTemero1, ClueBot NG, Jack Greenmaven, This lousy T-shirt, Thaumatropia, Widr, Matt j fox, Speedster3000, MerlIwBot, BG19bot, MarcMMMason, Aourangzaib, Lulzity, Alangar Manickam, Facilemindz, Dmaiolo, Contingentsecurity, Scopecreep, Artem12345, Wiki slav, Mr. Guye, Nic Cohen, RheaceJones, SFK2, Ofthehighest, Negus 69, MjadenSTEM, Maaxy, Sarac12345, Httpscard and Anonymous: 332
- **Physical security** *Source:* http://en.wikipedia.org/wiki/Physical%20security?oldid=634525604 *Contributors:* Mav, The Anome, Arvindn, William Avery, Edward, Nealmcb, Patrick, Dcljr, Ronz, Itai, Bearcat, Securiger, KellyCoinGuy, Lupo, Everyking, M0nde, Matt Crypto, TonyW, MattKingston, Wuzzeb, Notinasnaid, ZeroOne, LogicX, Graham87, BD2412, Stephenb, Grafen, Romal, Nikkimaria, GraemeL, Exit2DOS2000, SmackBot, Mmernex, C.Fred, Bluebot, Frap, Weregerbil, Quatloo, Kuru, Zapptastic, Beetstra, Tawkerbot2, Eastlaw, Shiseiji, Requestion, Cydebot, A876, Gogo Dodo, Dss311, Mattisse, AntiVandalBot, Barek, SiobhanHansa, VoABot II, McGov1258, CliffC, Jack007, Bus stop, Acalamari, Juliancolton, Red Thrush, NoticeBored, Jazzwick, Qxz, Trav123, Mazarin07, PatrickVSS, EverGreg, SecProf, Coffee, Steven hillard, Corp Vision, Pinkadelica, Nateusc, Zeerak88, Cptmurdok, Shustov, Alexbot, Tannchri, HumphreyW, Egmontaz, Dthomsen8, Mitch Ames, MystBot, Mojska, Ronhjones, LaaknorBot, Verbal, Legobot, Yobot, Andyj00, Magog the Ogre, AnomieBOT, Advancesafes55, Willowrock, Gabriel1907, Howwi, Ani.naran, Shadowjams, Prari, FrescoBot, 95j, Barras, Onel5969, CCTVPro, EmausBot, Lwlvii, Qrsdogg, Δ, Boundary11, Gloria06, Wipsenade, DanGelinas, Pastore Italy, ClueBot NG, Paperdown7132, Mesoderm, BG19bot, Sush 2252, Mitchitara, Securepro, Tentinator, Artelisys, JackDawsonHI, عراقي علي محمد, Dkwebsub, Monkbot and Anonymous: 96
- **Closed-circuit television** *Source:* http://en.wikipedia.org/wiki/Closed-circuit%20television?oldid=643472922 *Contributors:* AxelBoldt, The Anome, Alex, Ellmist, Zoe, Edward, Michael Hardy, Nixdorf, Pnm, Gabbe, Ixfd64, Arpingstone, Ahoerstemeier, Ronz, Theresa knott, Notheruser, Cadr, Timwi, Dysprosia, Daniel Quinlan, WhisperToMe, Radiojon, Morwen, Saltine, SEWilco, Scott Sanchez, Secretlondon, Finlay McWalter, Chuunen Baka, Robbot, ZimZalaBim, Postdlf, Danhuby, Kneiphof, Delpino, PBP, Alan Liefting, DocWatson42, Laudaka, Seabhcan, Orangemike, Mboverload, Solipsist, PlatinumX, Alvestrand, Tagishsimon, Chowbok, Utcursch, Alexf, Telso, LucasVB, Quadell, MacGyverMagic, Grauw, Rdsmith4, Glogger, Grimey, Máirtín, DMG413, Thorwald, Mike Rosoft, SimonEast, Freakofnurture, Gabriel vii, Bonalaw, Discospinster, Guanabot, YUL89YYZ, Night Gyr, ZeroOne, Violetriga, Zscout370, Aaronbrick, Richard Cane, Jonathan Drain, Dee Earley, La goutte de pluie, Ivansanchez, Matt tw, DCEdwards1966, Danski14, Anthony Appleyard, Duffman, Andrewpmk, Ricky81682, Lord Pistachio, SlimVirgin, Kotasik, Hu, Caesura, Coblin, Wtshymanski, Clubmarx, Yuckfoo, Dtcdthingy, Sfacets, Versageek, Drbreznjev, C3o, Woohookitty, Mindmatrix, WadeSimMiser, Acerperi, Isnow, Plrk, Jdorney, ThorstenS, Bilbo1507, Haikupoet, Jclemens, Mulligatawny, Dpr, Rjwilmsi, Koavf, Amire80, SMC, SNIyer12, SchuminWeb, RobertG, Ground Zero, Old Moonraker, Jrtayloriv, Quuxplusone, Srleffler, Zotel, Chobot, Bgwhite, UkPaolo, Borgx, MathiasRav, Briaboru, Stephenb, Gaius Cornelius, Elmaynardo, Rsrikanth05, Stassats, Amitabdev, Daveswagon, Danyoung, Irishguy, Aaron Brenneman, Jpbowen, Doctorindy, Xiroth, Htonl, Zzuuzz, Jacklee, Theda, Bd8494, Ydam, BorgQueen, GraemeL, Wbrameld, Fsiler, Archer7, Tall Midget, Thomas Blomberg, Mporcheron, Exit2DOS2000, Matthewmewtwo, SmackBot, CSMR, Zazaban, Reedy, McGeddon, Londonlinks, Finavon, Stifle, Edgar181, Direktorxxx, KYN, Portillo, Chris the speller, Oli Filth, MxAesir, DHN-bot, Colonies Chris, Madeinsane, Frap, Voyajer, Rrburke, Gwwfps, Kcordina, Jmlk17, Radagast83, Nakon, Valenciano, Dream out loud, James084, BrentRockwood, Jaqian, DMacks, Maelnuneb, Ricky@36, Ricky540, Will Beback, Kuru, John, SilkTork, Silkroad111, Jeffness, Ckatz, Hargle, Dicklyon, Crich1, Waggers, E-Kartoffel, Dennisw, Dean1970, TJ Spyke, BranStark, Fan-1967, Iridescent, J Di, Linkspamremover, JForget, Americasroof, CmdrObot, AlbertSM, Stephenjh, Jennifer Maddock, N2e, Gogo Dodo, Rick030391, Martin Jensen, Phydend, NorthernThunder, Ward3001, Lindsay658, Quartic, The machine512, DavidSteinle, HappyInGeneral, Trappleton, Jnorthup, MichaelMaggs, Dawnseeker2000, AntiVandalBot, Ais523, Gioto, Luna Santin, Ansett, Smartse, Spencer, Alphachimpbot, VictorAnyakin, Gerardkcohen, Amberroom, Ingolfson, JAnDbot, Fellix, Harryzilber, MER-C, Hartzz, Thenino, SiobhanHansa, SteveSims, Wildhartlivie, Akuyume, Magioladitis, Hroðulf, Pedro, Bongwarrior,

VoABot II, JamesBWatson, Doug Coldwell, Sdane02, KConWiki, Giggy, 28421u2232nfenfcenc, Cpl Syx, Glen, DerHexer, Simmo676, Waytohappiness, Fuseau, MartinBot, Prgrmr@wrk, Jim.henderson, Gowish, R'n'B, CommonsDelinker, Nono64, Worldedixor, J.delanoy, Trusilver, Dingdongalistic, PWdiamond, Maurice Carbonaro, Athaenara, NerdyNSK, Stressbattle, Dg2006, Thatotherperson, JayJasper, Plasticup, Whsecurity, Benthompson, Wespyu, Olegwiki, Juliancolton, Richardhaime, Gtg204y, TWCarlson, Mstubz, CardinalDan, Funandtrvl, VolkovBot, Scdweb, BeriCol, Lear's Fool, Philip Trueman, Bsiatadshmia, Shortstraw, Liamoliver, Technopat, Rebornsoldier, Ask123, Ajay.gaur, 2mcctv, Anna Lincoln, Seb26, CanOfWorms, LeaveSleaves, Snowbot, BotKung, Waycool27, Vipppa, Abigailhamilton, Andy Dingley, Norbu19, Falcon8765, Enviroboy, Turgan, Ulf Abrahamsson, Jhbarr, Securicorp, Pc9889, TimProof, Theoneintraining, LoveGirlsUK, SieBot, Madman, Jsc83, Lucasbfrbot, Hirohisat, A. Carty, Jojalozzo, Doritosyeah, Avnjay, Bennett92, Lightmouse, Hobartimus, Millstream3, AndrzejBania, Sqrtminusone, Capitalismojo, Sheps999, Mtaylor848, Pinkadelica, Rachelgoodwin, Benhutuk, ImageRemovalBot, WikipedianMarlith, ClueBot, Tuneman1958, Hustvedt, Soklapptdasnie, The Thing That Should Not Be, Vinniebar, Ewawer, CaNNoNFoDDa, Mild Bill Hiccup, Denna Haldane, Hal8999, Jwihbey, RafaAzevedo, Tiamat2, Kingrattus, CipherPixel, Alexbot, Socrates2008, The Founders Intent, Sun Creator, MickMacNee, Lunchscale, Veggiehead, Night-vision-guru, Thehelpfulone, Matthew Desjardins, Herbertbauer, Chaosdruid, Thingg, Bmfoste, Ellswore, French2080, DumZiBoT, Blammermouth, XLinkBot, Duncan, Mitch Ames, Asianeditor, Abdul2m, Nickbao, Sjnorton, CalumH93, Addbot, Joe sav5, Torontoro, Glane23, AndersBot, Chzz, Esasus, Tide rolls, Verbal, Gremney, Vanuan, Gary P88, Luckas-bot, Yobot, Fraggle81, Xpli2000, THEN WHO WAS PHONE?, AnomieBOT, Fatal!ty, Etan J. Tal, Piano non troppo, Willowrock, Materialscientist, Felyza, Zshallbetter, ArthurBot, TheAMmollusc, Termininja, KedaiCCTVdotcom, ChildofMidnight, CARBr6, Date delinker, Grim23, Gabriel1907, Zoom-Arrow, Thinkbig173, Justintheeditor, I-am-not-john, Rd144 1, Dougofborg, FrescoBot, Schuhpuppe, Tobby72, DXfactor, Weetoddid, Securitymax, Wireless Keyboard, HamburgerRadio, امیرشاهین, Pinethicket, I dream of horses, RPT01, Jonesey95, Jschnur, Kuyamarco123, Dougdoug2doug, Merlion444, FoxBot, Rootcctv, Hyasir123, PrimeauProductions, Knight in black satin, Wanne673, Alex k2, The Utahraptor, RjwilmsiBot, Espcctv, Jackehammond, Blaser508wen781, CCTVPro, IdealChain, Juni-dcctv, Barnettnews, Immunize, Nhajivandi, Zollerriia, Alirezatousi, Slightsmile, Wikipelli, Ahsirt, Mrbananaizsik, Khansaad, Timsellars1027, Cobaltcigs, Jpsammy, H3llBot, Obotlig, Jrest, Chrissimpson1987, MAGPIETRAP, Tsharples, Recca231, Jfiglik, Livypadre, Anjankolkata, Pastore Italy, Lisawaa, 2mcctv Cube, TYelliot, ClueBot NG, Jnorton7558, BarrelProof, Israa Sabha, Nantasatria, 05cnhh, Khan20021, Animusnovo, Muon, Mesoderm, O.Koslowski, ScottSteiner, Petey Parrot, Widr, Securitymedia, Tomreeve, Helpful Pixie Bot, Pdemaria, CCTVguru, BG19bot, Island Monkey, TheAdDorks, Toboboto, Wiki13, Hello9999, Lindapope, Shannahan15, Infocourse, Chmarkine, W charbonneau, I-80 Equipment, Kumaran.pondicherry, Megacolby, Tinkweb, Wikkiwitchh, Vanished user lt94ma34le12, KRoock74, SquallBLi, ChrisGualtieri, Khazar2, Triptakers, Artem12345, Artemlebedev34, Zim the invader, Vinjadhav, Isarra (HG), Threecreeksonetwothree, MiPeNo, 93, Comsat, Forrest1276, Wywin, RatiborNN, Burrito-Bazooka, Rjkrause, Roberts.stals, Jabedbablu, Advocatejake, Osmaantahir, Zenibus, Tls445, Quenhitran, Dator66, Whizz40, Intouchrugby, Crownespencer, RyDawg96, Demokra, Ian.moncur1997, Vitaltype, Clark Steph, Japanese Rail Fan, Monkbot, YdJ, Spitsyna91, Gordonsetlooe, Parktoy, Ggotero, Technokar and Anonymous: 681

- **Security guard** *Source:* http://en.wikipedia.org/wiki/Security%20guard?oldid=643892993 *Contributors:* Damian Yerrick, Brion VIBBER, SJK, Ortolan88, Ghakko, Roadrunner, Patrick, Ihcoyc, Furrykef, Saltine, HarryHenryGebel, Raul654, Scott Sanchez, Shantavira, Robbot, Icestryke, Donreed, Gidonb, Hadal, DocWatson42, Inter, Netoholic, Meursault2004, Henry Flower, Broux, Gyrofrog, Andycjp, Toytoy, Latitudinarian, Rlquall, Necrothesp, Benita, Neutrality, Davidstrauss, Safety Cap, Ulflarsen, Venu62, Moverton, Discospinster, Tomtom, ZeroOne, Shanes, Cmdrjameson, Zachlipton, Grutness, Andrewpmk, Lord Pistachio, ZeiP, Vuo, Computerjoe, BDD, Madmatt213, TShilo12, Matthew238, Feezo, Firsfron, Woohookitty, RHaworth, Tabletop, Dmol, Ozwegian, BD2412, Dwarf Kirlston, Rjwilmsi, Knave, Vegaswikian, Crazynas, NeonMerlin, SchuminWeb, Old Moonraker, Nivix, FeldBum, Random user 39849958, Vmenkov, Wavelength, Rtkat3, Thane, Anomalocaris, NawlinWiki, Retired username, Bd18packer, DeadEyeArrow, Kewp, Crisco 1492, 21655, Chase me ladies, I'm the Cavalry, Closedmouth, Spring Rubber, Airodyssey, Katieh5584, Fastifex, Exit2DOS2000, SmackBot, Looper5920, Andrew walker, Hydrogen Iodide, McGeddon, Mikecraig, Gjs238, Gilliam, Hmains, Chris the speller, Dolive21, Octahedron80, Can't sleep, clown will eat me, Factorylad, JRPG, OrphanBot, CelebritySecurity, SnappingTurtle, Dreadstar, RandomP, Tomtom9041, Gildir, Copysan, Captain Jason, JWaterman, MegaHasher, ShiningEyes, Gobonobo, Robdav69, Joffeloff, IronGargoyle, Noleander, OnBeyondZebrax, UncleDouggie, Igoldste, Chovain, Tawkerbot2, JeffJ, JForget, CmdrObot, Wafulz, Articnomad, GeorgeLouis, Gihanuk, Daland, Cahk, Hydraton31, NealIRC, Samuell, Gogo Dodo, Khatru2, Kevin23, ST47, Keruzin, Clovis Sangrail, Biggoggs, Optimist on the run, Gnfnrf, Ward3001, Ebraminio, Marina T., Thijs!bot, Pampas Cat, Mojo Hand, Oliver202, Missvain, Gasboys, Reswobslc, Dgies, Rhysis, F-451, Superzohar, Darklilac, Comakut, Barek, Rasseru, Rainingblood667, Independentassistant, Geniac, Kilrothi, VoABot II, JNW, Kja, Dep. Garcia, AIVEN, Catgut, Ali'i, Pps1, Justanother, RMP 2584, NJR ZA, Bobanny, DerHexer, WAAFFan1073977, Stanistani, Yhinz17, FisherQueen, Hdt83, Steamboat Willie, CliffC, Hairytoad2005, Windscar77, Raptorred04, Smokizzy, Mataharii, J.delanoy, Trusilver, Olaf Studt, Bogey97, Numbo3, Slow Riot, Privatemilitary, JBFrenchhorn, AntiSpamBot, Gregfitzy, Shoman93, Kraftlos, Something Original, Xiahou, Bnynms, Jeff G., Philip Trueman, Nkellof, Pmedema, Martin451, Abdullais4u, Jeremy Reeder, GodsKnight, Dpgtime, Mrug2, WJetChao, RaseaC, PatrickVSS, Legokid, StAnselm, Yintan, Manchurian, Ghostofme, Toddst1, Stimpy661, Decoratrix, Janggeom, StaticGull, Mygerardromance, Jdillingerceo, AltNet, Elassint, ClueBot, NickCT, Father Inire, The Thing That Should Not Be, Paul Trendall, Rodhullandemu, Bandurr, Dmvward, Yelruh, Place Clichy, Parkwells, Mr. Someguy, Thisglad, Excirial, OfficerCampbell, Zvrkljati, Parsival74, A plague of rainbows, Zxly, DumZiBoT, XLinkBot, WikHead, Mifter, Jmkim dot com, Dave1185, Addbot, Piz d'Es-Cha, Bouncertone, Yoenit, Nkolda, Geitost, Jncraton, Ironholds, Kongsinchi1976, Misterx2000, MrOllie, Aldrich Hanssen, Tide rolls, مانيم, Middayexpress, Yobot, Fraggle81, TaBOT-zerem, AnomieBOT, Kjambor, Jim1138, Piano non troppo, OakAshRiver, Materialscientist, Bagumba, LilHelpa, Anna Frodesiak, Kingdavy, ERhaught, Anime Addict AA, Wikieditor1988, 104Serena, Amaury, MerlLinkBot, Miru! Hajime desu!, Eugene-elgato, Awtanenbaum, FrescoBot, Bigtom98, Wikipe-tan, Ben Culture, Reddishwagon, Citation bot 1, Bklynkydd, Bobmack89x, Pinethicket, Halocandle, Degen Earthfast, John1234doe1234, Jonesey95, Fumitol, Wickelyby, And v, Inlandmamba, Tim1357, Graham2246, Jonkerz, Lotje, MistyPony1994, MrX, Reach Out to the Truth, Forcesecurityagency, Mean as custard, RjwilmsiBot, Ffffjjjj, Salvio giuliano, John of Reading, Fonda1, Mkirkendall, LAViking22, Tisane, Slightsmile, K6ka, Trideceth12, Illegitimate Barrister, Schemel, BushidoDevilDog, Hereforhomework2, H3llBot, Zoomrockr, L Kensington, Donner60, Pastore Italy, Ptts007, Cgtdk, E. Fokker, ClueBot NG, Robb hamic, MelbourneStar, Mchatton, Legionregional, Snotbot, Andrew Kurish, O.Koslowski, Widr, MerlIwBot, Markrylander, Nightenbelle, GuySh, Bmusician, Mfield8270, MusikAnimal, Feliciano17, Qbaby!!, Pooleinthehizzle, Snow Blizzard, KScarfone, Klilidiplomus, Sklarwiki, Michael Jaquish, Ghyath, Tubby12370, Khazar2, Basics31, Soni, Jjjjjjjjrrrrrrrr, Hmainsbot1, Mogism, MarPen, Disturbed88, Sreesarmatvm, Luke123lukeabc, Zaid231, Fatbuu1000, Xanco, UpstreamPaddler, SamX, Colleabois, Citobun, Sparkyb10123, SPSOA UNION, JaconaFrere, Djsisk, Sausage6969, WendigoUK, Trondandreass1 and Anonymous: 388

- **Separation barrier** *Source:* http://en.wikipedia.org/wiki/Separation%20barrier?oldid=642271113 *Contributors:* Bryan Derksen, Heron, Ja-

cobgreenbaum, Edward, Patrick, Liftarn, MartinHarper, Delirium, Ellywa, Angela, Kingturtle, JamesReyes, Uriber, Daniel Quinlan, Tris2000, Zero0000, Stormie, Hajor, ChrisO, Benwing, ZimZalaBim, Wereon, Casito, OneVoice, Argasp, Tom Radulovich, Iridium77, Bkonrad, Getback-world-respect, Zoney, Architeuthis, Kvasir, Eranb, Neutrality, Picapica, D6, Jayjg, Rich Farmbrough, Regebro, Stbalbach, GordyB, Kwamikagami, Jpgordon, TomStar81, Enric Naval, Cmdrjameson, Irishpunktom, Conny, Grutness, Eleland, Lectonar, Ynhockey, Max rspct, Bsadowski1, Instantnood, Bobrayner, Joriki, Mel Etitis, Bushytails, Woohookitty, Before My Ken, Wiki-vr, BD2412, Lasunncty, Reisio, Rjwilmsi, Koavf, Mitsukai, Kolbasz, Srleffler, Benlisquare, YurikBot, RussBot, GastelEtzwane, Van der Hoorn, Gaius Cornelius, Ksyrie, Gcapp1959, Lao Wai, CaliforniaAliBaba, Jove Is Mad, Chrishmt0423, GinaDana, Tsiaojian lee, Veinor, Big Adamsky, WookieInHeat, Bluebot, Sadads, Colonies Chris, Tewfik, Chlewbot, Slackermonkey, Rrburke, Khoikhoi, BIL, Derek R Bullamore, Das Baz, ILike2BeAnonymous, Kendrick7, Andeggs, SeattliteTungsten, Drork, Bless sins, AxG, Iridescent, Joseph Solis in Australia, Ewulp, Courcelles, Gilabrand, GeorgeLouis, Drinibot, Denis MacEoin, Avillia, Travelbird, DumbBOT, Mattisse, Diophantus, MesserWoland, S710, Niohe, Pie Man 360, Canadian, Carolmooredc, Alphachimpbot, RedCoat10, VoABot II, Dentren, CTF83!, Chesdovi, Nankai, Aristovoul0s, R'n'B, CommonsDelinker, Shawn in Montreal, Balthazarduju, KylieTastic, Alexander the Historian, Ottershrew, Black Kite, Meckanic, That-Vela-Fella, Wergmunt, Eblashko, Philip Trueman, Asarlaí, Andreas Kaganov, Soosim, Smashyourface86, Lucasbfrbot, Yintan, Not home, ZoRCoCuK, Lightmouse, ClueBot, Eeky, EoGuy, Heracletus, Saddhiyama, Mild Bill Hiccup, Rambler24, Taifarious1, DumZiBoT, XLinkBot, Emmette Hernandez Coleman, Maudemiller, Atoric, Addbot, Douglas the Comeback Kid, Floridianed, Hsteach, FrysUniverse, CountryBot, Yobot, Andreasmperu, MauriManya, Azylber, TestEditBot, AnomieBOT, Rkoala, Liqwid, Bumpymule, Eldeana, Makom55, Tjoshead, PJsantos, Lil-Helpa, Poetaris, Srich32977, J04n, Jalapenos do exist, MerlLinkBot, Asfarer, Friedlad, FrescoBot, Zukabovich, HCPUNXKID, Citation bot 1, Elockid, VanceCrowe, Jamescooly, Full-date unlinking bot, Reaper Eternal, Seahorseruler, Stalwart111, Kajervi, IRISZOOM, RjwilmsiBot, Gaia1CB3, Illegitimate Barrister, A930913, Greyshark09, Shrigley, Hang Li Po, Covington85, Cmckain, MerlIwBot, Lowercase sigmabot, BG19bot, Fangslayer, Darkness Shines, Abhimanyusa1, ÄDA - DÄP, Mogism, TippyGoomba, Sampa, Sandeeprao1, Jemkiranm, Jerry Pepsi, AnotherNewAccount, Monkbot, Tiptoethruthemineﬁeld, Knowledgebattle, Armouti0 0 and Anonymous: 127

- **Lock (security device)** *Source:* http://en.wikipedia.org/wiki/Lock%20(security%20device)?oldid=641407901 *Contributors:* Bryan Derksen, SimonP, Zanimum, Karada, Ronz, CatherineMunro, Adam Bishop, Przepla, Paul-L, Phoebe, Robbot, Chris 73, Lowellian, Sunray, Delpino, Robinh, Tobias Bergemann, Cedars, Varlaam, AlistairMcMillan, Antandrus, SeanProctor, Ojw, Jbinder, Jiy, Brianhe, Cacycle, Xezbeth, SocratesJedi, JemeL, ESkog, Aqua008, Bobo192, AmosWolfe, La goutte de pluie, Daf, Espoo, Coma28, Hohum, Vuo, Dennis Bratland, Pol098, WadeSimMiser, Tabletop, Clemmy, GregorB, Isnow, Jon Harald Søby, SqueakBox, Graham87, Fahrenheit451, Dimitrii, Yamamoto Ichiro, Jdeboer, Chobot, Roboto de Ajvol, YurikBot, Hairy Dude, RussBot, Conscious, Anomalocaris, NawlinWiki, Grafen, ONEder Boy, Zwobot, Wknight94, Zzuuzz, Chesnok, Closedmouth, Reyk, GraemeL, CWenger, JDspeeder1, NeilN, Tom Morris, Nick Michael, BRKey, Mach10, SmackBot, Herostratus, C.Fred, Jagged 85, Mirmo!, WookieInHeat, Gilliam, Ohnoitsjamie, Hmains, Armeria, Duozmo, Persian Poet Gal, Thumperward, Neo-Jay, Octahedron80, Arg, Darth Panda, Can't sleep, clown will eat me, Frap, Thisisbossi, VMS Mosaic, Addshore, Rekordronny, COMPFUNK2, KLLvr283, ML5, JHunterJ, Peter Horn, Areldyb, Courcelles, CmdrObot, Poloer, Green caterpillar, Slazenger, Cydebot, Samuell, Gogo Dodo, ST47, Odie5533, Tawkerbot4, SpK, Rosser1954, Thijs!bot, Epbr123, Ishdarian, Mojo Hand, Tellyaddict, Escarbot, AntiVandalBot, Brian Katt, JAnDbot, Agrestis, Sredna, Steveprutz, Acroterion, Bongwarrior, Dekimasu, Emelmujiro, Nikevich, Patstuart, Gun Powder Ma, Alx 91, MartinBot, Rettetast, R'n'B, Arriva436, J.delanoy, Pharaoh of the Wizards, Jan T. Kim, Mooreml, Acalamari, Ncmvocalist, McSly, TheTrojanHought, Rocket71048576, (jarbarf), Cyanide72, Rlfb, Pdcook, Idioma-bot, Funandtrvl, VolkovBot, Jeff G., Loxalot, Philip Trueman, TXiKiBoT, LeaveSleaves, Guldenat, Danny555, Mazarin07, Jamelan, The Devil's Advocate, AlleborgoBot, Milowent, Tvinh, EJF, SieBot, Joe4t, Jojalozzo, Hxhbot, Oxymoron83, Glederma, Lightmouse, ClueBot, Bigboy214, Babyboy808, Niceguyedc, Ericthehalfabone, Eeekster, Andriolo, Chipinnc, Cenarium, Audaciter, XDelv, Lambtron, Vanished user uih38riiw4hjlsd, Hotcrocodile, Dthomsen8, Ost316, SilvonenBot, Locknut1, Marchije, Exegete48, Addbot, Hrod84, Some jerk on the Internet, Jncraton, Ka Faraq Gatri, Freemasonx, Favonian, Farmercarlos, West.andrew.g, Jaypaww83, Tide rolls, Gail, English Lock, Yobot, TaBOT-zerem, Specious, Thangcuoi, EricWester, Retro00064, Mullassery, Synchronism, AnomieBOT, Jim1138, Mintrick, Bluerasberry, FRAC, OllieFury, ChristianH, Obersachsebot, Cureden, WmLawson, Asdfghjkl1412, Markus oosaies, Pinhead111, Clemensmarabu, RibotBOT, Kcdtsg, Alexandru Stanoi, Aashaa, Dartheragon1, Chipmunk2, Josemanimala, Photnart, FrescoBot, Sethary11, Bombtech86, Finalius, Javert, YourBoba, Jokester420j000005, I dream of horses, Elockid, Edderso, LittleWink, RyokoUri, MastiBot, Σ, Xeworlebi, Ravensburg13, Gamewizard71, Lotje, Vrenator, TheLongTone, Aiken drum, JV Smithy, Nazzzux, Sirkablaam, MoveableBeast, DARTH SIDIOUS 2, TjBot, Jackehammond, Galloping Moses, RA0808, Safes4you, Tommy2010, TuHan-Bot, Wikipelli, P. S. F. Freitas, Josve05a, Ahears, Truethmaster, Dictionary199, Caspertheghost, Noodleki, Puffin, Carmichael, ChuispastonBot, Beatles-Ramones, Tacotown, Xanchester, ClueBot NG, MelbourneStar, Satellizer, Dhanor, Jb3141, Isaiah1038, TruPepitoM, Sirgabe, Ali ringo, Nathanholder, Dgratz, MerlIwBot, Ramaksoud2000, Krishnaprasaths, Furkhaocean, Whoisthatclown, Juro2351, Yankeefan0395, ISTB351, Clive.morley, Ilove2pickongeorgewashington, Jawadreventon, Duende-Poetry, RscprinterBot, Mae1209, Breakthelock, Wojcikgang, Webclient101, Mogism, Amdin2, TwoTwoHello, BlueRoll18, Fycafterpro, Philbert mc pie, Idk what u call me, Kogmaw, Mhbeals, Powermaster55, Alexis101beast, Liamiscool2132, Speedlocksmith, SylvyRaves, Bloggz1, COOLCUB01, Lagoset, Fakeaccount54321, Joel padilla1978, Wikibl007, John685, Wwmray, Sarac12345 and Anonymous: 269

- **Access control** *Source:* http://en.wikipedia.org/wiki/Access%20control?oldid=637278291 *Contributors:* Timo Honkasalo, The Anome, Edward, Patrick, BAxelrod, Wikiborg, Vaceituno, Texture, Auric, Tobias Bergemann, Alan Liefting, Andycjp, Omassey, Bderidder, CHoltje, El C, Sietse Snel, BrokenSegue, SPUI, Espoo, Hu, Wtmitchell, Dave.Dunford, Neetij, H2g2bob, Ringbang, Woohookitty, Mindmatrix, Camw, Daira Hopwood, Jeff3000, PeregrineAY, BD2412, Rjwilmsi, Amire80, Nicolas1981, Eubot, Old Moonraker, Nihiltres, Gurch, Intgr, Chobot, DVdm, Bgwhite, Borgx, RussBot, Stephenb, Gaius Cornelius, NawlinWiki, Grafen, Welsh, PrologFan, Auminski, Galar71, Ka-Ping Yee, Back ache, Guinness man, DEng, Carlosguitar, Exit2DOS2000, SmackBot, McGeddon, Zzm7000, Xaosflux, Delfeye, Silly rabbit, DHN-bot, Frap, RoyalBlueStuey, Andreiij, Trbdavies, Luís Felipe Braga, Chris0334, ArielGlenn, Kuru, Yan Kuligin, Twredfish, Slakr, E-Kartoffel, Thatcher, Kvng, Hu12, Hetar, MikeHobday, Linkspamremover, CmdrObot, Cydebot, Gogo Dodo, Jedonnelley, Soifranc, QuiteUnusual, MER-C, NE2, Roleplayer, Knokej, Magioladitis, McGov1258, George A. M., Web-Crawling Stickler, Americanhero, Billbl, FisherQueen, Bostonvaulter, CliffC, CommonsDelinker, Fmjohnson, Memoroid, Hersfold, Philip Trueman, TXiKiBoT, SecurityEditor, Ziounclesi, Mazarin07, Andy Dingley, Scouttle, EverGreg, Nickbernon, Wikiscottcha, SieBot, Therepguy, Happysailor, Brankow, Lightmouse, Sfan00 IMG, ClueBot, Josang, Binksternet, Apacheguru, DragonBot, LadyAngel89, Eldub1999, The Founders Intent, Dekisugi, Aitias, Talsetrocks, Wsimonsen, Pichpich, Tonypdmtr, Mitch Ames, MystBot, RyanCross, Addbot, Actatek, Leszek Jańczuk, Fluffernutter, Rickfray, Subverted, Stantry, مانې, Gail, Jarble, Ben Ben, Luckas-bot, Yobot, Bunnyhop11, KamikazeBot, Timothyhouse1, AnomieBOT, Advancesafes55, Piano non troppo, Willowrock, Materialscientist, StewartNetAddict, Securitywiki, Sionk, Jgeorge60, Andriusval, SassoBot, Kernel.package, Jray123, Ruuddekeijzer, Indyaedave, Nageh,

Mark Renier, DrilBot, Winterst, Swamy.narasimha, Testplt75, Jandalhandler, Lotje, Vrenator, Clarkcj12, Zeeshankhuhro, Lingliu07, Mean as custard, EmausBot, WikitanvirBot, Timtempleton, Immunize, Feptel, Iancbend, Gagandeeps117, Abhinavcambridge, Josve05a, Krd, Iwatch-webmaster, RISCO Group, Ssbabudilip, Dineshkumar Ponnusamy, ChuispastonBot, ClueBot NG, Sesha Sayee K V, KunjanKshetri, Chester Markel, Secguru1, Animusnovo, Mesoderm, Stewartjohnson229900, Widr, Ellerose, BG19bot, The Illusive Man, Cfeltus, Codename Lisa, Vinjadhav, TheSadnessOfBeing, David.brossard, Dewoller, Fan Zhang-IHC, Luesand, Mattgavenda, TotaliTech, Mumbui, Weikrx, Mgavenda, Rsschomburg, Virgo hariom, Clark Steph, Cmontgomery11, Cybersecurity101, Filedelinkerbot, Ggotero, Hphaikuku, Thetechgirl, Zubairul and Anonymous: 240

- **Alarm device** *Source:* http://en.wikipedia.org/wiki/Alarm%20device?oldid=620998827 *Contributors:* Vicki Rosenzweig, Mav, Patrick, Egil, Mac, TUF-KAT, GCarty, Gepwiki, Robbot, Chris 73, PBP, BenFrantzDale, DX, Andycjp, HorsePunchKid, Srbauer, Spalding, Anthony Appleyard, Wtmitchell, Drbreznjev, Nuno Tavares, Lupinelawyer, Eras-mus, Dacs, YurikBot, Borgx, Ryansworld100000, Stephenb, Ugur Basak, Wknight94, Exit2DOS2000, SmackBot, Gilliam, Carl.bunderson, Hraefen, Bluebot, Geneb1955, Sadads, Drjackzon, Can't sleep, clown will eat me, Unrevealing, COMPFUNK2, Anoopkn, Weregerbil, E-Kartoffel, Bwpach, Shoeofdeath, Neelix, Roberta F., Thijs!bot, Ufwuct, LachlanA, AntiVandalBot, JAnDbot, Carlwev, Saburny, VolkovBot, DRAGON Elemental, StacyMGA, Bentogoa, Oxymoron83, Correogsk, Cyfal, Billsalt, ClueBot, Connor.carey, GERMSGOL, The Founders Intent, Addbot, CarsracBot, CUSENZA Mario, Luckas-bot, Yobot, Willowrock, ArthurBot, Landfritter, Joxemai, Erik9bot, D'ohBot, Tretyak, RedBot, BjörnBergman, AvocatoBot, Codename Lisa, LighthouseSecurity and Anonymous: 50
- **Motion detection** *Source:* http://en.wikipedia.org/wiki/Motion%20detection?oldid=639547605 *Contributors:* Kku, Selket, ZimZalaBim, Pne, Lucky 6.9, Quota, NetBot, Kappa, La goutte de pluie, Diego Moya, Seans Potato Business, Alex '05, Zsero, Wtshymanski, JeremyA, Waldir, BD2412, Quiddity, Siddhant, YurikBot, RussBot, Shaddack, Emana, Abune, KnightRider, SmackBot, Rizzardi, Chlewbot, Radagast83, Steve Pucci, Ithizar, Maelnuneb, Vina-iwbot, Clicketyclack, Anlace, Beetstra, Alan.ca, Aktalo, Dancter, Lindsay658, Thijs!bot, Dawnseeker2000, Orionus, Voortle, Alphachimpbot, Hello32020, R'n'B, Kovo138, SisterGool, 2verb, Jojalozzo, Axel.mulder, Quinacrine, ClueBot, The Thing That Should Not Be, Arjayay, SchreiberBike, Egmontaz, XLinkBot, Doughywilson, Kjellgro, Pataki Márta, Addbot, SpBot, Jarble, Luckas-bot, Yobot, RIAL org, RibotBOT, SmilyAJ, ChrstphrChvz, Pelham88, DennisIsMe, Tot12, NTox, Milad Mosapoor, Event Nexus, ClueBot NG, Kalyan.akella, CaroleHenson, Helpful Pixie Bot, Dacs uk, Lgalescu, Arcanoroma, Keone.kahananui, Rajath87 and Anonymous: 77
- **Glass break detector** *Source:* http://en.wikipedia.org/wiki/Glass%20break%20detector?oldid=621089716 *Contributors:* Echoray, Devtrash, Henry Flower, Rich Farmbrough, Phlake, PdDemeter, Uncle G, Kbdank71, Rjwilmsi, SchuminWeb, Alynna Kasmira, GraemeL, SmackBot, Science3456, Frap, Dicklyon, Amalas, Cydebot, MarshBot, Magioladitis, Javawizard, Dg2006, Afluegel, Belovedfreak, Funandtrvl, VolkovBot, AlfonZ42, EverGreg, Wdwd, The Founders Intent, Addbot, Ptbotgourou, AnomieBOT, Tristantech, Wipsenade, ClueBot NG and Anonymous: 14
- **Identity document** *Source:* http://en.wikipedia.org/wiki/Identity%20document?oldid=643560659 *Contributors:* The Anome, Walter, SimonP, Patrick, Dante Alighieri, Gabbe, Fwappler, CesarB, Snoyes, Darkwind, Error, Bogdangiusca, Jiang, Cheeni, Ec5618, RickK, Snickerdo, Wik, LMB, Vaceituno, Scott Sanchez, Trevor mendham, David.Monniaux, Donarreiskoffer, Bearcat, Dale Arnett, Jez f, ChrisO, Chrism, RedWolf, Altenmann, DHN, Halibutt, Bkell, Kostiq, Ninjamask, Smjg, MaGioZal, DavidCary, Andromeda, Mintleaf, Seabhcan, Meursault2004, Lupin, Timpo, Orpheus, Trujaman, JimD, Alensha, Mboverload, Zoney, Apoivre, VampWillow, Avala, Pne, Bobblewik, Jurema Oliveira, Chowbok, Utcursch, Quadell, Antandrus, OwenBlacker, Heirpixel, Necrothesp, Huaiwei, Cab88, Bonalaw, Discospinster, Brianhe, MCBastos, Pie4all88, ArnoldReinhold, YUL89YYZ, JohnRDaily, Michael Zimmermann, Lordscissorhand, CanisRufus, Livajo, Gilgamesh he, CXI, Art LaPella, Coolcaesar, Nwerneck, Sortior, SpeedyGonsales, Hawklord, La goutte de pluie, BenM, Wrs1864, 24.123..., Keriluamox, Orzetto, Molteanu, Transfinite, DenisHowe, Rd232, Zippanova, Denniss, Danaman5, EAi, Egg, Vuo, Kusma, Alai, Instantnood, HenryLi, Ceyockey, Killing Vector, Novacatz, Scarykitty, Boothy443, Richard Arthur Norton (1958-), OwenX, Woohookitty, Mindmatrix, David Haslam, SunTzu2, James Kemp, Davidkazuhiro, Tabletop, GregorB, John Hill, Meelosh, Doco, Mayz, Gimboid13, MD, Brownsteve, Icydid, Gerbrant, Mandarax, Deltabeignet, BD2412, Rjwilmsi, Angusmclellan, Leeyc0, Xanderall, Tawker, X1011, Vegaswikian, DoubleBlue, Cassowary, BradCuppy, SNIyer12, Baldwin.jim, FayssalF, FlaBot, Nonsequiturmine, Naraht, DDerby, SchuminWeb, RexNL, Lmatt, Atitarev, LOCALHOST, Dtruslove, Energy, Diamantina, Chobot, Sherool, Benlisquare, The One True Fred, Bgwhite, Gwernol, Wavelength, RobotE, Hairy Dude, Kardosbalint, Huw Powell, Dannycas, Kymacpherson, RussBot, Tryforceful, Apancu, Bill Statler, Gaius Cornelius, Phil-hong, Txuspe, Bullzeye, The Ogre, Joel7687, R'son-W, Adamrush, Nick, Brian Crawford, Moe Epsilon, Marshall, Juras14, Chichui, Htonl, Lockesdonkey, JoshFarron, Tachs, Phaedrus86, Wknight94, Kelovy, Daniel C, J S Ayer, Cassius1213, Coolgene, Petri Krohn, GraemeL, LeonardoRob0t, Mais oui!, NFH, Smurfy, Whouk, Buybooks Marius, Co149, AndrewWTaylor, MacsBug, SmackBot, Unschool, Estoy Aquí, Aiman abmajid, Iamajpeg, The Monster, Gnangarra, Bomac, Aseismic, Stifle, Willicher, Flamarande, Mtahir, Septegram, Eiler7, D39, Gilliam, 9591353082, Jushi, Chris the speller, Reza1615, Flurry, TheSpectator, Mdwh, FalconZero, William Allen Simpson, Jmax-, Brideshead, Famspear, EaglesFanInTampa, John C PI, Tuxley, Gibnews, BIL, MrRadioGuy, Nakon, Derek R Bullamore, Dantadd, Wizardman, Mojo-chan, Ohconfucius, PeterNisbet, Takamaxa, Flip619, Jidanni, Tazmaniacs, Heimstern, Park3r, Rundquist, Joffeloff, Stefan2, Bjankuloski06en, Drork, QDE-can, MaximvsDecimvs, Beetstra, WELCOME PEOPLE, Cnis, Santa Sangre, TastyPoutine, Sijo Ripa, Jggouvea, Barbiedrag, Hu12, Nehrams2020, Dead3y3, Iridescent, Joseph Solis in Australia, Sander Säde, Goran.S2, ChemicalBit, Tawkerbot2, Nydas, Shahbz, Zahn, HDCase, CRGreathouse, CmdrObot, GeorgeLouis, NaBUru38, Requestion, CoolCityCat, The Photographer, EdmundWong, Sgt Simpson, Cydebot, Diegom809, Abeg92, Future Perfect at Sunrise, Gogo Dodo, David Moss, Kozuch, Biruitorul, Nachdenklich, Berria, WilliamH, Legnaw, MPorciusCato, JustAGal, Grayshi, I already forgot, Linuxprophet, AntiVandalBot, JurgenG, Tmopkisn, Superzohar, Shelgason, Spartaz, Aranho, JAnDbot, AniRaptor2001, MER-C, Byeee, Gazilion, Joshua, Zorro CX, Geniac, KEKPΩΨ, Magioladitis, Adegirmenci, VoABot II, Nevermind1534, Maheshkumaryadav, Notaryone, BanRay, Katrin Laas, Dima1, Goldfish007, Genius babak, Afil, Stephenchou0722, Jackson Peebles, Johnbevan, BetBot, Amarand, Rettetast, R'n'B, CommonsDelinker, Ervinet, Manticore, Neolandes, Terrek, Chtrede, Svidrillion, Mikael Häggström, Skier Dude, Mjb1981, AntiSpamBot, Plasticup, Nippymippy, Ahuskay, Phirazo, Binba, Olegwiki, Fattonysaysyes, DQJK2000, Nbinr1, RVJ, W. Frank, Idioma-bot, Pietru, Negemo, Jollyjoegiant, Law Lord, Sk741, Campuscodi, Chrisieboy, Wiikipedian, LeaveSleaves, Christopher Connor, One half 3544, Bonus bon, Fraxinus Croat, Majalinno, Tri400, Adam.J.W.C., Falcon8765, Iwoolf, Andres65, Munci, S.Örvarr.S, Mcintireallen, Dan Polansky, The Red Hat of Pat Ferrick, Tony2621, WereSpielChequers, Rave92, Argentineboy, Paulbrock, Mr Taz, Quest for Truth, Eido.inoue, Infestor, David Be, ZoRCoCuK, Topher385, Egrian, Nicksname, Xeltran, Spitfire19, Jaimiethedog, Dodger67, Tesi1700, Ossæ, Denisarona, Npd2983, ImageRemovalBot, Dlrohrer2003, Jsdixie, ClueBot, NickCT, Kl4m, Tcfinley, Snigbrook, Rayyung, Fyyer, Plastikspork, RashersTierney, Ewawer, Wysprgr2005, Drmies, Sevilledade, Mild Bill Hiccup, Guerreroivanb, Niceguyedc, ElSaxo, Auntof6, Alice, Excirial, TheMagicalMuffin, Mfa fariz, Editorbloke1900, Sun Creator, L.tak, Iohannes Animosus, Philip200291, Undyne, Mlaffs, TheTranc, 2, BalkanFever, DumZiBoT, YXN,

Nick in syd, Olybrius, Bud08, Dthomsen8, Lstanley1979, WikHead, Alexius08, Intracndnt, Allinadayswork, Easyteddy, Riohadzic, Marc CAT, Mlavic, Hawkania, Addbot, User1389, Mootros, Douglas the Comeback Kid, Download, Zwyciezca, Pyl, Rekyht101, Komischn, Lightbot, Teles, Shikuesi3, Yobot, Gabrielsouza15, TaBOT-zerem, Hilanin, Sc3821, Alakasam, Gerixau, Nikidp, Againme, AnomieBOT, A More Perfect Onion, Rjanag, Dwayne, Kingpin13, Cossde, Abshirdheere, EryZ, Okisdwed, Flewis, Pella01, Identnmb, LilHelpa, Tom.magnussen, Jtorres875, Gymnophoria, Stoichkov8, 4twenty42o, Kareersoft786, Sir Stanley, S11.1, Cerniagigante, بیووی ا, Kikodawgzzz, Alblefter, Corollo12, Lordvisucius, Dedltd, EastExpert, FrescoBot, Mark Renier, Thayts, Pizzagrill, Cody Cooper, Gourami Watcher, HamburgerRadio, Zulhelpme, Ondokuzmart, Koogel moogel, RedBot, Dianagospodaru, Jujutacular, Full-date unlinking bot, Awae196, Samuel Salzman, Orenburg1, Trappist the monk, Ayzeen, Tareq.sami, Lotje, Harald Meier, Begoon, ZhBot, Abelikus, IRISZOOM, DARTH SIDIOUS 2, Eustanacio IV, RjwilmsiBot, TortoretoTom, Kingsland71, EmausBot, John of Reading, Dolescum, Zollerriia, Dewritech, Ultracold, Security King, Wikipelli, AsceticRose, Thecheesykid, Splibubay, Shuipzv3, BWP1234, Mar4d, Zwbookworm, Keskitalo, Cardprinter, H3llBot, SporkBot, Gz33, Erianna, RaptureBot, Δ, KazekageTR, Markiewp, Donner60, Hypethral, TruckCard, Bundawda, 28bot, ClueBot NG, ClaretAsh, MelbourneStar, Kais0989, Satellizer, Michalplsko, Luckypaperarmen, Yasser ELH, Frietjes, Aight 2009, Gaas99, Tc.edit, Spel-Punc-Gram, Finding-Truth, Doma93, MerlIwBot, BG19bot, Dharshana.l.h, Bmusician, Phương Huy, ZebraMonkey, Shujenchang, Albatalab, Supernerd11, Mtmoore321, Wikitorrens, Caldodekevin, Katangais, Ubiquinoid, Nestor.mcnab, Pratyya Ghosh, ArcadiaID, ChrisGualtieri, Khazar2, Soulparadox, JonyDAG, Esszet, SeleMG, Mogism, Triomio, Jemappelleungarcon, Johnjay1745, JustAMuggle, Samee, Andber08, Belowerapid Zhang, Epicgenius, Rob984, Swungscener, Harlem Baker Hughes, Danielwhitehorn, Rekowo, Noyster, SantiaguitoIII, Albatalad, Souffront17, Monkbot, Merispollar, Samuelcolvin, Nelson serrao and Anonymous: 676

- **Alarm management** *Source:* http://en.wikipedia.org/wiki/Alarm%20management?oldid=642452773 *Contributors:* Pekkapihlajasaari, Smack, Phil Boswell, Caknuck, DavidCary, CALR, CanisRufus, RoyBoy, CDN99, Themusicgod1, Spalding, Famousdog, Wtshymanski, Limegreen, Siddhant, Byron Vickers, Stephenb, Vdegroot, Nelson50, MacsBug, SmackBot, Sadads, Soap, RomanSpa, E-Kartoffel, Joseph Solis in Australia, Brian.neufeld, Jac16888, Wordbuilder, Matthewshepherd, InvertRect, Sean herringuk, AlanHugo, Martin Hollender, Supersteve04038, Kyle the bot, EverGreg, SoManySpammers, Arthur Smart, Paulnarmad, WillemHazenberg, Mild Bill Hiccup, Addbot, Asmeditor, AnomieBOT, Smapple, Citation bot, Msmarmalade, LilHelpa, J04n, GWS EE, Bbaeck, Lpstegman, EdoDodo, Twhubbert, RjwilmsiBot, Hirsutism, Akjar13, Josve05a, ClueBot NG, Asmwebadmin, Hamish59, Ruudtim, Igx-pr, InvictaSystems and Anonymous: 33
- **Door security** *Source:* http://en.wikipedia.org/wiki/Door%20security?oldid=640342080 *Contributors:* Edward, Discospinster, Gene Nygaard, Alvis, RHaworth, Tslocum, Wavelength, Dhollm, Nikkimaria, Exit2DOS2000, SmackBot, Brianski, Flurry, Frap, Caleb Murdock, Twredfish, Minna Sora no Shita, AlbertaSunwapta, Seekmage, P199, Courcelles, Dalahäst, MER-C, Flowanda, Idioma-bot, Thomas.W, Koussouros, Brankow, Ronaldoreeder, Sfan00 IMG, OldManClemens33, Addbot, Favonian, Avneshsh429, Yobot, AnomieBOT, Max Cheung, FrescoBot, Mauricio Duque, Killian441, Mean as custard, ZéroBot, Speedster3000, Manishk.mosaic, Loriendrew, Cerabot, Magnolia677, Costa.stewart, Noyster, Cherrybsw, Bishalbaishya2012, Toolbin.cc and Anonymous: 45
- **Guard tour patrol system** *Source:* http://en.wikipedia.org/wiki/Guard%20tour%20patrol%20system?oldid=615298913 *Contributors:* ALE!, Avihu, Brianhe, Triona, Jeodesic, Atlant, MONGO, BD2412, Nightscream, CJLL Wright, Zafiroblue05, Gaius Cornelius, DragonHawk, Exit2DOS2000, SmackBot, Maelwys, Rockpocket, Bollinger, EricR, JeffJ, ShelfSkewed, Justanother, LorenzoB, Enviroboy, Guoguo12, Ernie n08, Tony2am, The Evil IP address, Armbrust, Connectgroup, Timur1505, EdoBot, Joefromrandb, Mark Arsten, H8usernames, F.preller, Monkbot and Anonymous: 10
- **Security engineering** *Source:* http://en.wikipedia.org/wiki/Security%20engineering?oldid=634415749 *Contributors:* Robert Merkel, The Anome, Dwheeler, Scott, The Anomebot, Enigmasoldier, Selket, Tpbradbury, Korath, Sverdrup, Giftlite, Matt Crypto, Ablewisuk, Andreas Kaufmann, D6, ArnoldReinhold, El C, Grutness, Arthena, Neonumbers, Suruena, SteinbDJ, Commander Keane, Graham87, BD2412, Josh Parris, Vegaswikian, Gurch, Wimt, SamJohnston, Jpbowen, Ospalh, Whouk, Exit2DOS2000, That Guy, From That Show!, SmackBot, Mmernex, Mauls, Frap, CelebritySecurity, Kcordina, FrankWilliams, Imecs, Lambiam, Twredfish, Peter Horn, Neelix, A876, Lotte Monz, Ljean, Manionc, Ingolfson, WLU, R'n'B, JA.Davidson, Tonyshan, Shamatt, Ross Fraser, Remi0o, TreasuryTag, Philip Trueman, Sjfield, Rlendog, Mikebar, Jojalozzo, Sfan00 IMG, ClueBot, Shustov, Excirial, PixelBot, Mywikicontribs, David stokar, SilvonenBot, Pbjason9, Wyatt915, MrOllie, Debresser, Tassedethe, Legobot, Luckas-bot, Yobot, OrgasGirl, Baldbunny619, Sweerek, AnomieBOT, Willowrock, Citation bot, AllThatJazz65, Crzer07, SCΛRECROW, FrescoBot, Jonkerz, RjwilmsiBot, EmausBot, H3llBot, Secpert, S Larctia, Codename Lisa, يقاراعلا يلع دمحم, Jonathan lampe, Mknayeri2000 and Anonymous: 51
- **Surveillance** *Source:* http://en.wikipedia.org/wiki/Surveillance?oldid=643198776 *Contributors:* AxelBoldt, Derek Ross, WojPob, The Anome, Ortolan88, DavidLevinson, Edward, Patrick, Michael Hardy, Kku, Liftarn, Suisui, Kingturtle, Michael Shields, Tristanb, Mxn, Novum, Dysprosia, WhisperToMe, Wik, Hyacinth, Nv8200p, David.Monniaux, MrJones, ZimZalaBim, Securiger, Lowellian, Chris Roy, Vfrickey, Michael Snow, Mushroom, Zigger, Solipsist, Tagishsimon, Andycjp, Popefauvexxiii, Beland, Glogger, Toshimarise, Izzycohen, N328KF, Discospinster, Rich Farmbrough, Bender235, ZeroOne, JoeSmack, Pedant, JustPhil, El C, Kwamikagami, Leif, Adambro, Harley peters, ZayZayEM, Arcadian, Csabo, Babajobu, Paleorthid, Ejstarchuk, Efortune, Hu, Hohum, Evil Monkey, ~shuri, Bookandcoffee, Walshga, Hq3473, Richard Arthur Norton (1958-), Alvis, Woohookitty, Pol098, Mangojuice, Stefanomione, Clapaucius, Canderson7, Rjwilmsi, PHenry, Wingover, G Clark, Ground Zero, Old Moonraker, Jrtayloriv, Quuxplusone, Coolhawks88, YurikBot, Wavelength, RussBot, Hede2000, Raquel Baranow, Hydrargyrum, Stephenb, Gaius Cornelius, Shaddack, Rsrikanth05, Nirvana2013, Aeusoes1, Joel7687, JulesH, SeaFox, Zzuuzz, Jacklee, Petri Krohn, GraemeL, Ajuk, Izayohi, Veinor, MacsBug, SmackBot, Mmernex, Moez, Impaciente, McGeddon, J-beda, Londonlinks, Alex earlier account, Jdfoote, Ohnoitsjamie, Snappa, Chris the speller, Spilla, Oli Filth, Victorgrigas, Scwlong, Chendy, Can't sleep, clown will eat me, Frap, MJBurrage, OOODDD, Gala.martin, COMPFUNK2, YankeeDoodle14, Badgerpatrol, Weregerbil, Ohconfucius, Byelf2007, Quevaal, J 1982, Gobonobo, Ckatz, A. Parrot, Beetstra, E-Kartoffel, Nabeth, Hu12, OnBeyondZebrax, Kencf0618, Agent X2, K0Yaku, Joseph Solis in Australia, Dp462090, Linkspamremover, Tawkerbot2, Chetvorno, Jafet, ChrisCork, CmdrObot, ShelfSkewed, Sdorrance, Bakanov, Myasuda, Drozdp, Cydebot, Mike Christie, Gogo Dodo, Optimist on the run, Maziotis, Thijs!bot, Epbr123, Maximilian Schönherr, PaperTruths, Tobias Baccas, Classic rocker, Dawnseeker2000, AntiVandalBot, Gioto, Mashiah Davidson, Alphachimpbot, Guul, CGroup, Yancyfry jr, Res2216firestar, JAnDbot, Deflective, MER-C, SiobhanHansa, Elizabennet, Magioladitis, Bongwarrior, VoABot II, Atalanta86, Soulbot, Nyttend, Froid, Eysen, MCG, DerHexer, WLU, Foregone conclusion, Waytohappiness, Atulsnischal, Jim.henderson, GeorgHH, Évangéline, TheEgyptian, CommonsDelinker, Balaraat, J.delanoy, Jcsurveillance, Siobhan Hansa, Jesant13, Brian Pearson, Olegwiki, Xavier Giró, Scranium, TRimester6, Diamondrake, Concaire, Foofighter20x, Ogranut, Sandman619, Scdweb, IHTFP, Crevox, GcSwRhIc, Humair85, Aymatth2, Qxz, PeetMoss, Free0willy, Doc James, Nicksoda21, Interstates, Swliv, Spease, Csblack, Doritosyeah, Moonraker12, Brankow, Mazugrin, RW Marloe, Slmvbs, Svick, Joel Rennie,

ClueBot, Mingacorn91, Bigdoole, Tanglewood4, Mild Bill Hiccup, Laudak, SuperHamster, CoolIdeas, Abrech, Rhododendrites, Erunestian, Night-vision-guru, Ellswore, DumZiBoT, Maraparacc, AlanM1, XLinkBot, Abdul2m, Zodon, Activenanda, Addbot, Ashton1983, Download, Sillyfolkboy, Ccacsmss, Tassedethe, MagneH, Wireless friend, Jarble, Tartarus, Artichoke-Boy, Yobot, Granpuff, Alexanderhayes, Fraggle81, TaBOT-zerem, Edoe, Kikbguy, AnomieBOT, Decora, A Taste of Terre Haute, Rjanag, Piano non troppo, Quantumseven, Mahmudmasri, Materialscientist, Jcs45, Mechamind90, LilHelpa, Mlduda, Xqbot, PhDOnPoint, Capricorn42, Tnyl, ToLLIa, Gabriel1907, Tulaneadam21, Shadowjams, FrescoBot, Citation bot 1, Pinethicket, Rochdalehornet, Merlion444, Videoinspector, Zevschonberg, Sociologo11, Clirmion, RjwilmsiBot, Davegagner, DexDor, CCTVPro, Wunderpants, EmausBot, John of Reading, Super48paul, Contributor75, Smurfjones, Jenks24, Nyenten, H3llBot, Exhibitions.intern, W163, Jrest, Madisonpadre, ClueBot NG, Mesoderm, Tjepsen, Helpful Pixie Bot, Mdeets, BG19bot, Slater555, Northamerica1000, Wiki13, Paganinip, Elzaibak, MrSidneyReilly, Meclee, Glacialfox, Tristan Lall, Michaelpetercarter, Chrisswanger, BattyBot, Jimw338, Cyberbot II, Khazar2, E.N.Stanway, Artem12345, IjonTichyIjonTichy, The kaper, Stacy Jacobson, Shivajivarma, Mathfreak231, Yulipipin, Donnchacol, Bravoa60, Ugog Nizdast, Watchpocket, Whizz40, Dodi 8238, Petelogger, Danniel Curze, Ibrahim Farid, Monkbot, Parktoy, Chrisnlorenzo and Anonymous: 271

16.9.2 Images

- **File:1-Wire_lock.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c0/1-Wire_lock.jpg *License:* CC-BY-SA-3.0 *Contributors:* Own work *Original artist:* Stan Zurek
- **File:2010-04-06_Security_guard.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/00/2010-04-06_Security_guard.jpg *License:* GFDL *Contributors:* Own work *Original artist:* Ildar Sagdejev (Specious)
- **File:2010-05-14-USCYBERCOM_Logo.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/3a/2010-05-14-USCYBERCOM_Logo.jpg *License:* Public domain *Contributors:* Department of Defense *Original artist:* http://www.defense.gov/home/features/2010/0410_cybersec/images/cybercom_seal_large1.jpg Department of Defense
- **File:ACT_Provisional_Drivers_Licence_2009.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/8b/ACT_Provisional_Drivers_Licence_2009.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Benlisquare
- **File:ADT_Bel-Air_Patrol_Vehicle.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e7/ADT_Bel-Air_Patrol_Vehicle.jpg *License:* CC BY-SA 3.0 *Contributors:* Transferred from en.wikipedia; transferred to Commons by User:Kafuffle using CommonsHelper. *Original artist:* Something Original (talk). Original uploader was Something Original at en.wikipedia
- **File:Access_control_door_wiring.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/10/Access_control_door_wiring.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_door_wiring_io_module.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f2/Access_control_door_wiring_io_module.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_IP_controller.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/5b/Access_control_topologies_IP_controller.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_IP_master.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/95/Access_control_topologies_IP_master.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_IP_reader.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/ef/Access_control_topologies_IP_reader.png *License:* Public domain *Contributors:* Midpoint Systems, UAB *Original artist:* Andriusval
- **File:Access_control_topologies_main_controller_a.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/8f/Access_control_topologies_main_controller_a.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_main_controller_b.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/a5/Access_control_topologies_main_controller_b.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_serial_controllers.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e0/Access_control_topologies_serial_controllers.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Access_control_topologies_terminal_servers.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/ac/Access_control_topologies_terminal_servers.png *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Alexis_Navy_Yard_012_1dsLQLVk7nY.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/78/Alexis_Navy_Yard_012_1dsLQLVk7nY.jpg *License:* Public domain *Contributors:* http://www.youtube.com/ *Original artist:* United States Department of the Navy (CCTV), United States federal government, Federal Bureau of Investigation
- **File:Ambox_globe_content.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/b/bd/Ambox_globe_content.svg *License:* Public domain *Contributors:* Own work, using File:Information icon3.svg and File:Earth clip art.svg *Original artist:* penubag
- **File:Ambox_important.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/b/b4/Ambox_important.svg *License:* Public domain *Contributors:* Own work, based off of Image:Ambox scales.svg *Original artist:* Dsmurat (talk · contribs)
- **File:Ancient_warded_lock_key_transparent.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/33/Ancient_warded_lock_key_transparent.png *License:* CC BY-SA 3.0 *Contributors:*
- Ancient_warded_lock_key.jpg *Original artist:* Ancient_warded_lock_key.jpg: Pethrus
- **File:BIPT.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/1e/BIPT.jpg *License:* Public domain *Contributors:* Scanned by myself from my own document *Original artist:* User:Dantadd
- **File:Bansky_one_nation_under_cctv.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/8a/Bansky_one_nation_under_cctv.jpg *License:* CC BY-SA 2.0 *Contributors:* One Nation Under CCTV *Original artist:* oogiboig

- **File:Berlin_Schönefeld_Airport_metal_detectors.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f7/Berlin_Sch%C3%B6nefeld_Airport_metal_detectors.jpg *License:* GFDL *Contributors:* ? *Original artist:* ?
- **File:Berlinermauer.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/5d/Berlinermauer.jpg *License:* CC-BY-SA-3.0 *Contributors:* http://de.wikipedia.org/wiki/Datei:Bethanien06.jpg
  Original artist: Noir
- **File:Borderbeachtj.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/d/df/Borderbeachtj.jpg *License:* Public domain *Contributors:* Transferred from en.wikipedia
  Original artist: JamesReyes at en.wikipedia
- **File:Bosnian_ID_card_B.gif** *Source:* http://upload.wikimedia.org/wikipedia/en/f/f4/Bosnian_ID_card_B.gif *License:* CC-BY-3.0 *Contributors:*

  I created this work entirely by myself.

  Original artist:

  FaceOffic (talk)
- **File:Boundless_Informant_data_collection.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/5b/Boundless_Informant_data_collection.svg *License:* CC0 *Contributors:* Own work This file was derived from: BlankMap-World6.svg
  Original artist: Rezonansowy
- **File:Bulgarian_identity_card.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/83/Bulgarian_identity_card.png *License:* Public domain *Contributors:* http://prado.consilium.europa.eu/en/5437/viewImage_153828.html *Original artist:* Bulgarian Government
- **File:Bulger_cctv.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/6/62/Bulger_cctv.jpg *License:* Fair use *Contributors:*

  This image is a still taken from a shopping centre CCTV camera in 1993. It was released by the shopping centre to the police and the public in the hunt for James Bulger's killers. It is contended to be in the public domain. The specific image (with a border) was taken from the BBC News website.

  Original artist:

  unknown
- **File:CIA.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/23/CIA.svg *License:* Public domain *Contributors:* http://www.law.cornell.edu/uscode/50/403m.html *Original artist:* United States federal government
- **File:Cairns-Lagoon.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/a4/Cairns-Lagoon.JPG *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia; transferred to Commons by User:Bidgee using CommonsHelper. *Original artist:* Original uploader was Frances76 at en.wikipedia
- **File:Canadian_Embassy_DC_2007_002.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/83/Canadian_Embassy_DC_2007_002.jpg *License:* Public domain *Contributors:* Own work *Original artist:* Gryffindor
- **File:Carta_identita_italiana.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/24/Carta_identita_italiana.jpg *License:* CC-BY-SA-3.0 *Contributors:* Transferred from it.wikipedia *Original artist:* Original uploader was Gaspardo85 at it.wikipedia
- **File:Cedula_Antigua_de_Venezuela.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/4f/Cedula_Antigua_de_Venezuela.jpg *License:* CC0 *Contributors:* Own work *Original artist:* Wilfredor
- **File:Chinese_lock.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/97/Chinese_lock.JPG *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Clemensmarabu
- **File:ChippedSerbianID_face.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f4/ChippedSerbianID_face.png *License:* Public domain *Contributors:* http://www.mup.gov.rs/cms_lat/dokumenta.nsf/licna-karta-specimen.h *Original artist:* Republic of Serbia, Ministry of Interior.
- **File:Chubb_lock.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/24/Chubb_lock.jpg *License:* Public domain *Contributors:* http://www.oldlocks.com/lockpicking.htm *Original artist:* Unknown
- **File:Ciuru.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/02/Ciuru.jpg *License:* GPL *Contributors:* ? *Original artist:* ?
- **File:Closed.circuit.camera.arp.750pix.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c5/Closed.circuit.camera.arp.750pix.jpg *License:* Public domain *Contributors:* Originally from en.wikipedia; description page is/was here. *Original artist:* Arpingstone at English Wikipedia
- **File:Columbine_Shooting_Security_Camera.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/d/de/Columbine_Shooting_Security_Camera.jpg *License:* Fair use *Contributors:*

  http://3.bp.blogspot.com/-qg80gh7NVa4/TbrhvLAuJkI/AAAAAAAAACg/o8IVkcatPv0/s1600/columbine%2Bshooting.jpg *Original artist:* ?
- **File:Commons-logo.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:ConstellationGPS.gif** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/9c/ConstellationGPS.gif *License:* Public domain *Contributors:* Transferred from en.wikipedia *Original artist:* Original uploader was El pak at en.wikipedia
- **File:Crystal_Clear_app_kedit.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e8/Crystal_Clear_app_kedit.svg *License:* LGPL *Contributors:* Sabine MINICONI *Original artist:* Sabine MINICONI
- **File:DNIArg-anv-wikipedia.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/ce/DNIArg-anv-wikipedia.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Ojota
- **File:DNI_peruano.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/2e/DNI_peruano.jpg *License:* Public domain *Contributors:* Own work *Original artist:* Wikiperuvian

- **File:DSTAMP_Controp_Camera.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/b/bb/DSTAMP_Controp_Camera.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* 320i
- **File:Delta_World_HQ_-_entrance_with_security_station.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/94/Delta_World_HQ_-_entrance_with_security_station.JPG *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Mav
- **File:Digital_video_recorder.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/47/Digital_video_recorder.jpg *License:* Public domain *Contributors:* Own work *Original artist:* Rd144 1
- **File:Disc_tumbler_locked.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/00/Disc_tumbler_locked.png *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia *Original artist:* Original uploader was Wapcaplet at en.wikipedia
- **File:Dome_CCTV_cameras.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/45/Dome_CCTV_cameras.JPG *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* KRoock74
- **File:Dowodos.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/73/Dowodos.png *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:EXAMPLEVENEZUELANID.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/87/EXAMPLEVENEZUELANID.jpg *License:* CC BY-SA 3.0 *Contributors:* scanned by me *Original artist:* JonyDAG
- **File:Edit-clear.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/f/f2/Edit-clear.svg *License:* Public domain *Contributors:* The *Tango! Desktop Project*. *Original artist:*

  The people from the Tango! project. And according to the meta-data in the file, specifically: "Andreas Nilsson, and Jakub Steiner (although minimally)."
- **File:Emergency-Locksmith-Brooklyn.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/7f/Emergency-Locksmith-Brooklyn.jpg *License:* CC0 *Contributors:* http://nyclocksmithbrooklyn.com/ *Original artist:* Locksmithwilli
- **File:Eye-in-the-sky083.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/0f/Eye-in-the-sky083.jpg *License:* CC-BY-SA-3.0 *Contributors:* Originally from en.wikipedia; description page is/was here. *Original artist:* Original uploader was Glogger at en.wikipedia
- **File:FN_polis_vid_COP15_i_Kopenhamn_2009.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/1f/FN_polis_vid_COP15_i_Kopenhamn_2009.jpg *License:* CC BY 2.5 dk *Contributors:* Nordic Co-operation website (norden.org), http://www.norden.org/en/news-and-events/images/events/others/cop15-2009/fn-polis/view *Original artist:* Johannes Jansson
- **File:Flag_of_Australia.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/b/b9/Flag_of_Australia.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Canada.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/c/cf/Flag_of_Canada.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Flag_of_France.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/c/c3/Flag_of_France.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Germany.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/b/ba/Flag_of_Germany.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Flag_of_New_Zealand.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/3e/Flag_of_New_Zealand.svg *License:* Public domain *Contributors:* http://www.mch.govt.nz/files/NZ%20Flag%20-%20proportions.JPG *Original artist:* Zscout370, Hugh Jass and many others
- **File:Flag_of_the_United_Kingdom.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/a/ae/Flag_of_the_United_Kingdom.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Fob-at-proximity-reader_532_130xauto.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/cf/Fob-at-proximity-reader_532_130xauto.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work Template:Self photograph Template:Http://www.accesscontrol.ie/products/category/pro/ *Original artist:* Mgavenda
- **File:Folder_Hexagonal_Icon.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/4/48/Folder_Hexagonal_Icon.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:GBM-passiv.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f6/GBM-passiv.jpg *License:* GFDL *Contributors:* Own work *Original artist:* Echoray
- **File:Greek_ID_Card-Back.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/6/6a/Greek_ID_Card-Back.jpg *License:* Public domain *Contributors:* Ελληνικό Υπουργείο Δημοσίας Τάξης Εικόνα *Original artist:* Ελληνικό Υπουργείο Δημοσίας Τάξης
- **File:Greek_ID_Card-Front.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/02/Greek_ID_Card-Front.jpg *License:* Public domain *Contributors:* Ελληνικό Υπουργείο Δημοσίας Τάξης Εικόνα *Original artist:* Ελληνικό Υπουργείο Δημοσίας Τάξης
- **File:Green_Line_near_Paphos_Gate.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/98/Green_Line_near_Paphos_Gate.JPG *License:* CC-BY-SA-3.0 *Contributors:* Own work, transferred by SalopianJames from English Wikipedia where filename was en:File:PHOT0093.JPG *Original artist:* User:Little firefly
- **File:Guangzhou-Cash-transport-0454.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/2b/Guangzhou-Cash-transport-0454.jpg *License:* CC-BY-SA-3.0 *Contributors:* Own work (Own photo) *Original artist:* User:Vmenkov
- **File:HKID_pic-adult-front_sample.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/2/23/HKID_pic-adult-front_sample.jpg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:HK_Security001.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e5/HK_Security001.jpg *License:* CC-BY-SA-3.0 *Contributors:* Own work (Original text: *self-made*) *Original artist:* Kongsinchi1976 (talk)

- **File:HURT_concept_drawing.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e9/HURT_concept_drawing.jpg *License:* Public domain *Contributors:* http://www.darpa.mil/ipto/programs/hart/hart_vision.asp *Original artist:* Wikipedia: DARPA / Wikipedia: Information Processing Technology Office
- **File:HunIDback.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/3b/HunIDback.jpg *License:* CC BY 3.0 *Contributors:* Own work *Original artist:* me
- **File:HunIDfront.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/9d/HunIDfront.jpg *License:* CC-BY-SA-3.0 *Contributors:* Own work *Original artist:* me
- **File:IAO-logo.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/d/d1/IAO-logo.png *License:* Public domain *Contributors:* Transferred from en.wikipedia; transfered to Commons by User:Papa November using CommonsHelper. *Original artist:* Original uploader was Kwertii at en.wikipedia
- **File:ID-card-spain-(01).png** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/23/ID-card-spain-%2801%29.png *License:* CC SA 1.0 *Contributors:* ? *Original artist:* ?
- **File:IDCard_PK.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/2/29/IDCard_PK.jpg *License:* Cc-by-sa-3.0 *Contributors:*

  own

  Original artist:

  me
- **File:ID_card_SVK.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/31/ID_card_SVK.JPG *License:* Public domain *Contributors:* Own work *Original artist:* Legnaw
- **File:Idrou.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/25/Idrou.jpg *License:* Public domain *Contributors:* self-scanned *Original artist:* ?
- **File:Integrated_LCD_DVR.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/0a/Integrated_LCD_DVR.jpg *License:* Public domain *Contributors:* Transferred from en.wikipedia; transfer was stated to be made by User:Rockfang. *Original artist:* Original uploader was Kingrattus at en.wikipedia
- **File:Intelligent_access_control_door_wiring.PNG** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/53/Intelligent_access_control_door_wiring.PNG *License:* Public domain *Contributors:* Own work *Original artist:* Andriusval
- **File:Intellinet_Network_Solutions_NSC11-WN_Home_Network_IP_Camera.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/ad/Intellinet_Network_Solutions_NSC11-WN_Home_Network_IP_Camera.jpg *License:* ? *Contributors:* http://www.intellinet-network.com/en-US/products/9316-nsc11-wn-network-camera *Original artist:* Intellinet Network Solutions
- **File:Israel_Batch_1_(889).JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c1/Israel_Batch_1_%28889%29.JPG *License:* Public domain *Contributors:* Own work *Original artist:* User:Mattes
- **File:Jumin_shenfenzheng.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/6/68/Jumin_shenfenzheng.jpg *License:* CC BY 2.5 *Contributors:* Own work *Original artist:* Coolgene
- **File:Kathmandu-05.JPG** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/21/Kathmandu-05.JPG *License:* CC-BY-SA-3.0 *Contributors:* Own work *Original artist:* Sigismund von Dobschütz
- **File:Kencf0618FacebookNetwork.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/90/Kencf0618FacebookNetwork.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Kencf0618
- **File:Kenyan_security_officer.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/2e/Kenyan_security_officer.jpg *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:Leternjoftimi_shqiptar_biometrik...jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/d/d5/Leternjoftimi_shqiptar_biometrik...jpg *License:* Public domain *Contributors:* Transferred from en.wikipedia to Commons by SreeBot. *Original artist:* Alblefter at en.wikipedia
- **File:Locking_mechanism_on_box_recovered_from_the_Vasa.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c6/Locking_mechanism_on_box_recovered_from_the_Vasa.jpg *License:* CC BY-SA 3.0 *Contributors:* ? *Original artist:* ?
- **File:Locks_CPK.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/6/62/Locks_CPK.jpg *License:* CC0 *Contributors:* Own work *Original artist:* Лапоть
- **File:Locksmiths-11211.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/7a/Locksmiths-11211.jpg *License:* CC0 *Contributors:* http://nyclocksmithbrooklyn.com/security-systems/fast-locksmith-anytime-locks/ *Original artist:* Locksmithwilli
- **File:Lorex_digital_wireless_camera.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/e/ef/Lorex_digital_wireless_camera.jpg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Macedonian_id.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/f/f1/Macedonian_id.jpg *License:* CC-BY-SA-3.0 *Contributors:*

  self-made

  Original artist:

  Cukiger (talk)
- **File:Mendel_I_072_v.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/83/Mendel_I_072_v.jpg *License:* Public domain *Contributors:* Hausbuch der Mendelschen Zwölfbrüderstiftung, Band 1. Nürnberg 1426–1549. Stadtbibliothek Nürnberg, Amb. 317.2°, via http://www.nuernberger-hausbuecher.de/ *Original artist:* Anonymous
- **File:Mergefrom.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/0f/Mergefrom.svg *License:* Public domain *Contributors:* ? *Original artist:* ?

- **File:MicroAirVehicle.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/03/MicroAirVehicle.jpg *License:* Public domain *Contributors:* Cropped and balanced from [1] at [2] *Original artist:* w:United States Navy photo by Mass Communication Specialist 3rd Class Kenneth G. Takada
- **File:Montenegrin_identity_card.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/77/Montenegrin_identity_card.jpg *License:* Public domain *Contributors:* http://www.gov.me/vijesti.php?akcija=vijesti&id=153055 *Original artist:* Montenegro, Ministry of Interior
- **File:Montreal_Security_2009_067.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/73/Montreal_Security_2009_067.jpg *License:* Public domain *Contributors:* Own work *Original artist:* MontrealSecurity2002
- **File:Mr._Richard_R._Chaney.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/ab/Mr._Richard_R._Chaney.jpg *License:* ? *Contributors:* Flickr: Mr. Richard R. Chaney *Original artist:* Smithsonian Institution
- **File:Mustermann_nPA.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f6/Mustermann_nPA.jpg *License:* Public domain *Contributors:* Transferred from de.wikipedia; transfer was stated to be made by User:Komischn. *Original artist:* Bundesrepublik Deutschland, Bundesministerium des Innern.
- **File:National_Security_Agency.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/0/04/National_Security_Agency.svg *License:* Public domain *Contributors:* www.nsa.gov *Original artist:* U.S. Government
- **File:NewYorkCitySubwayEntranceInterior.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/55/NewYorkCitySubwayEntranceInterior.jpg *License:* CC BY 3.0 *Contributors:* Own work *Original artist:* Canadaolympic989
- **File:Nuvola_apps_kcmsystem.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/7a/Nuvola_apps_kcmsystem.svg *License:* LGPL *Contributors:* Own work based on Image:Nuvola apps kcmsystem.png by Alphax originally from [1] *Original artist:* MesserWoland
- **File:Nuvola_apps_ksim.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/8d/Nuvola_apps_ksim.png *License:* LGPL *Contributors:* http://icon-king.com *Original artist:* David Vignoni / ICON KING
- **File:Osobna_iskaznica_2013_-_prednja_strana.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/79/Osobna_iskaznica_2013_-_prednja_strana.jpg *License:* Public domain *Contributors:* http://www.mup.hr/71.aspx *Original artist:* Croatian government
- **File:Paypass_chip_front.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c8/Paypass_chip_front.png *License:* GFDL *Contributors:* ? *Original artist:* ?
- **File:Persoonskaart.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/16/Persoonskaart.jpg *License:* CC BY 2.5 *Contributors:* ? *Original artist:* ?
- **File:Physical_security_access_control_with_a_fingerprint_scanner.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/8b/Physical_security_access_control_with_a_fingerprint_scanner.jpg *License:* CC BY 3.0 *Contributors:* Own work *Original artist:* Lgate74
- **File:Pin_tumbler_no_key.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e8/Pin_tumbler_no_key.svg *License:* CC-BY-SA-3.0 *Contributors:* File:Cilinderslot gesloten.png *Original artist:* Original: GWirken; Derivative work: Pbroks13
- **File:Portal-puzzle.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/f/fd/Portal-puzzle.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Private_factory_guard.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f7/Private_factory_guard.jpg *License:* CC BY 2.0 *Contributors:* Flickr.com - image description page *Original artist:* Robbie Sproule from Montreal, Canada
- **File:Private_security_workers_in_Johannesburg_during_World_Cup_2010-06-29_2.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/b/b5/Private_security_workers_in_Johannesburg_during_World_Cup_2010-06-29_2.jpg *License:* CC BY 3.0 br *Contributors:* agenciabrasil.ebc.com.br *Original artist:* Marcello Casal Jr/ABr
- **File:QLD_Proof_of_Age_Card.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/22/QLD_Proof_of_Age_Card.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Shujenchang
- **File:Question_book-new.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*

  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:*

  Tkgd2007
- **File:RFID_hand_1.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/99/RFID_hand_1.jpg *License:* CC BY-SA 2.0 *Contributors:* ? *Original artist:* ?
- **File:Security_guard_in_China_01.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/26/Security_guard_in_China_01.jpg *License:* CC0 *Contributors:* Own work *Original artist:* Anna Frodesiak
- **File:Security_spikes_1.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/e4/Security_spikes_1.jpg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Social_Security_card.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/11/Social_Security_card.jpg *License:* Public domain *Contributors:* http://waysandmeans.house.gov/legacy/images/socseccard.jpg *Original artist:* Social Security Administration
- **File:Standing_Guard.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c9/Standing_Guard.jpg *License:* Public domain *Contributors:* http://www.filestube.com/6Gveb6baIsdLxqLvPb4QJo/105-Old-India-in-Paintings-Wallpapers-Collection-zip.html *Original artist:* Rudolf Ernst
- **File:Sur-veillance-trafficcam-glog.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/e/eb/Sur-veillance-trafficcam-glog.jpg *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia *Original artist:* Original uploader was Glogger at en.wikipedia

- **File:SurveillanceCamera2.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/fc/SurveillanceCamera2.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Dator66
- **File:SurveillanceCamera4.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f5/SurveillanceCamera4.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Dator66
- **File:Surveillance_cameras_mapped.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/6/64/Surveillance_cameras_mapped.png *License:* CC0 *Contributors:* Own work *Original artist:* Windsock92
- **File:Surveillance_quevaal.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/9/98/Surveillance_quevaal.jpg *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:Surveillance_video_cameras,_Gdynia.jpeg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/30/Surveillance_video_cameras%2C_Gdynia.jpeg *License:* CC BY 2.5 *Contributors:* Own work *Original artist:* Paweł Zdziarski
- **File:Symbol_book_class2.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/89/Symbol_book_class2.svg *License:* CC BY-SA 2.5 *Contributors:* Mad by Lokal_Profil by combining: *Original artist:* Lokal_Profil
- **File:THE_CENTRAL_POLICE_CONTROL_STATION,_MANNED_24_HOURS_A_DAY_CONTROLS_ALL_TRAFFIC_LIGHTS,_RECEIVES_REMOTE_TV_INPUTS_FROM..._-_NARA_-_551905.tif** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/5c/THE_CENTRAL_POLICE_CONTROL_STATION%2C_MANNED_24_HOURS_A_DAY_CONTROLS_ALL_TRAFFIC_LIGHTS%2C_RECEIVES_REMOTE_TV_INPUTS_FROM..._-_NARA_-_551905.tif *License:* Public domain *Contributors:* U.S. National Archives and Records Administration *Original artist:* Yoichi R. (Yoichi Robert) Okamoto, 1915-, Photographer (NARA record: 2987665)
- **File:TaiwanIDCard_jchung.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/7/73/TaiwanIDCard_jchung.jpg *License:* GFDL *Contributors:* ? *Original artist:* ?
- **File:TaiwanID_backside.jpg** *Source:* http://upload.wikimedia.org/wikipedia/en/9/9f/TaiwanID_backside.jpg *License:* PD *Contributors:* Author
  Original artist:
  User:Jchungkana
- **File:Text_document_with_red_question_mark.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/a4/Text_document_with_red_question_mark.svg *License:* Public domain *Contributors:* Created by bdesham with Inkscape; based upon Text-x-generic.svg from the Tango project. *Original artist:* Benjamin D. Esham (bdesham)
- **File:The_separation_barrier_which_runs_through_Bethlehem.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/3f/The_separation_barrier_which_runs_through_Bethlehem.jpg *License:* CC BY 2.0 *Contributors:* Bethlehem *Original artist:* Trocaire from Ireland
- **File:Three_Surveillance_cameras.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/a/a1/Three_Surveillance_cameras.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Hustvedt
- **File:Tubular_locked.png** *Source:* http://upload.wikimedia.org/wikipedia/commons/8/84/Tubular_locked.png *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:US-CentralSecurityService-Seal.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/6/6a/US-CentralSecurityService-Seal.svg *License:* Public domain *Contributors:* Extracted from PDF version of 50th Anniversary Brochure (direct PDF URL [1]). *Original artist:* U.S. Government
- **File:US-DeptOfJustice-Seal.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/2/26/US-DeptOfJustice-Seal.svg *License:* Public domain *Contributors:* Extracted from PDF file available here. *Original artist:* U.S. government
- **File:US-FBI-ShadedSeal.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/7/70/US-FBI-ShadedSeal.svg *License:* Public domain *Contributors:* Extracted from PDF version of a DNI 100-day plan followup report (direct PDF URL here). *Original artist:* Federal Bureau of Investigation
- **File:US-VISIT_(CBP).jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/5/5c/US-VISIT_%28CBP%29.jpg *License:* Public domain *Contributors:* U.S. Customs and Border Protection photographic archives (image permalink) *Original artist:* Gerald Nino/CPB
- **File:US_Department_of_Homeland_Security_Seal.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/4c/US_Department_of_Homeland_Security_Seal.svg *License:* Public domain *Contributors:* http://www.uscg.mil/ *Original artist:* DHS, as noted below.
- **File:US_Navy_050308-N-2385R-029_Master-at-Arms_Seaman_Carly_Farmer_checks_an_identification_card_(ID)_before_allowing_a_driver_to_enter_the_gate_at_U.S._Fleet_Activities_Sasebo,_Japan.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/42/US_Navy_050308-N-2385R-029_Master-at-Arms_Seaman_Carly_Farmer_checks_an_identification_card_%28ID%29_before_allowing_a_driver_to_enter_the_gate_at_U.S._Fleet_Activities_Sasebo%2C_Japan.jpg *License:* Public domain *Contributors:*
  This Image was released by the United States Navy with the ID 050308-N-2385R-029 (next).
  This tag does not indicate the copyright status of the attached work. A normal copyright tag is still required. See Commons:Licensing for more information.
  Original artist: U.S. Navy photo by Photographer's Mate 3rd Class Yesenia Rosas
- **File:UncleSamListensIn.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/46/UncleSamListensIn.jpg *License:* CC BY 2.0 *Contributors:* https://secure.flickr.com/photos/jeffschuler/2585181312/in/set-72157604249628154 *Original artist:* Jeff Schuler
- **File:Video_surveillance_sign.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/4/47/Video_surveillance_sign.jpg *License:* CC-BY-SA-3.0 *Contributors:* Originally from en.wikipedia; description page is/was here. *Original artist:* Original uploader was Quadell at en.wikipedia

- **File:Wfm_cctv_van.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/c/c8/Wfm_cctv_van.jpg *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:Whampoa_Garden_security_post.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/3/35/Whampoa_Garden_security_post.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Citobun
- **File:Wiki_letter_w.svg** *Source:* http://upload.wikimedia.org/wikipedia/en/6/6c/Wiki_letter_w.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Wiki_letter_w_cropped.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/1c/Wiki_letter_w_cropped.svg *License:* CC-BY-SA-3.0 *Contributors:*
- Wiki_letter_w.svg *Original artist:* Wiki_letter_w.svg: Jarkko Piiroinen
- **File:Wikibooks-logo-en-noslogan.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/d/df/Wikibooks-logo-en-noslogan.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wiktionary-logo-en.svg** *Source:* http://upload.wikimedia.org/wikipedia/commons/f/f8/Wiktionary-logo-en.svg *License:* Public domain *Contributors:* Vector version of Image:Wiktionary-logo-en.png. *Original artist:* Vectorized by Fvasconcellos (talk · contribs), based on original logo tossed together by Brion Vibber
- **File:Xatta137.jpg** *Source:* http://upload.wikimedia.org/wikipedia/commons/1/1c/Xatta137.jpg *License:* Attribution *Contributors:* Own work *Original artist:* Ori~

16.9.3 Content license