WIKIPEDIA

Mass surveillance

Mass surveillance is the intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens.[1] The surveillance is often carried out by local and federal governments or governmental organisations, such as organizations like the NSA and the FBI, but it may also be carried out by corporations (either on behalf of governments or at their own initiative). Depending on each nation's laws and judicial systems, the legality of and the permission required to engage in mass surveillance varies. It is the single most indicative distinguishing trait of totalitarian regimes. It is also often distinguished from targeted surveillance.

Mass surveillance has often been cited as necessary to fight terrorism, prevent crime and social unrest, protect national security, and control the population. Conversely, mass surveillance has equally often been criticized for violating privacy rights, limiting civil and political rights and freedoms, and being illegal under some legal or constitutional systems. Another criticism is that increasing mass surveillance could lead to the development of a surveillance state or an electronic police state where civil liberties are infringed or political dissent is undermined by COINTELPRO-like programs. Such a state could be referred to as a totalitarian state.

In 2013, the practice of mass surveillance by world[2] governments was called into question after Edward Snowden's 2013 global surveillance disclosure. Reporting based on documents Snowden leaked to various media outlets triggered a debate about civil liberties and the right to privacy in the Digital Age.[3] Mass surveillance is considered a global issue.[4][5][6][7]

Contents

By country

Privacy International's 2007 survey, covering 47 countries, indicated that there had been an increase in surveillance and a decline in the performance of privacy safeguards, compared to the previous year. Balancing these factors, eight countries were rated as being 'endemic surveillance societies'. Of these eight, China, Malaysia and Russia scored lowest, followed jointly by Singapore and the United Kingdom, then jointly by Taiwan, Thailand and the United States. The best ranking was given to Greece, which was judged to have 'adequate safeguards against abuse'.[8]

Many countries throughout the world have already been adding thousands of surveillance cameras to their urban, suburban and even rural areas.[9][10] For example, in September 2007 the American Civil Liberties Union (ACLU) stated that we are "in danger of tipping into a genuine surveillance society completely alien to American values" with "the potential for a dark future where our every move, our every transaction, our every communication is recorded, compiled, and stored away, ready to be examined and used against us by the authorities whenever they want."[11]

On 12 March 2013, Reporters Without Borders published a *Special report on Internet Surveillance*. The report included a list of "State Enemies of the Internet", countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. Five countries were placed on the initial list: Bahrain, China, Iran, Syria, and Vietnam.[12]

Australia

Bahrain

Bahrain is one of the five countries on Reporters Without Borders' March 2013 list of "State Enemies of the Internet", countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. The level of Internet filtering and surveillance in Bahrain is one of the highest in the world. The royal family is represented in all areas of Internet management and has sophisticated tools at its disposal for spying on its subjects. The online activities of dissidents and news providers are closely monitored and the surveillance is increasing.[12]

Canada

China

China is one of the five countries on Reporters Without Borders' March 2013 list of "State Enemies of the Internet", countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. All Internet access in China is owned or controlled by the state or the Communist Party. Many foreign journalists in China have said that they take for granted that their telephones are tapped and their email is monitored.[12]

The tools put in place to filter and monitor the Internet are collectively known as the Great Firewall of China. Besides the usual routing regulations that allow access to an IP address or a particular domain name to be blocked, the Great Firewall makes large-scale use of Deep Packet Inspection (DPI) technology to monitor and block access based on keyword detection. The Great Firewall has the ability to dynamically block encrypted connections. One of the country's main ISPs, China Unicom, automatically cuts a connection as soon as it is used to transmit encrypted content.[12]

The monitoring system developed by China is not confined to the Great Firewall, monitoring is also built into social networks, chat services and VoIP. Private companies are directly responsible to the Chinese authorities for surveillance of their networks to ensure banned messages are not circulated. The QQ application, owned by the firm Tencent, allows the authorities to monitor in detail exchanges between Internet users by seeking certain keywords and expressions. The author of each message can be identified by his or her user number. The QQ application is effectively a giant Trojan horse. And since March 2012, new legislation requires all new users of micro-blogging sites to register using their own name and telephone number.[12]

Skype, one of the world's most popular Internet telephone platforms, is closely monitored. Skype services in China are available through a local partner, the TOM media group. The Chinese-language version of Skype, known as TOM-Skype, is slightly different from the downloadable versions in other countries. A report by OpenNet Initiative Asia[13] says everyday conversations are captured on servers. Interception and storage of a conversation may be triggered by a sender's or recipient's name or by keywords that occur in the conversation.[14]

On 30 January, the *New York Times* reported that it had been the target of attacks by the Chinese government. The first breach took place on 13 September 2012 when the newspaper was preparing to publish an article about the fortune amassed by the family of outgoing Prime Minister Wen Jiabao. The newspaper said the purpose of attacks was to identify the sources that supplied the newspaper with information about corruption among the prime minister's entourage. The *Wall Street Journal* and *CNN* also said they had been the targets of cyber attacks from China. In February, Twitter disclosed that the accounts of some 250,000 subscribers had been the victims of attacks from China similar to those carried out on the *New York Times*. Mandiant, the company engaged by the NYT to secure its network, identified the source of the attacks as a group of hackers it called Advanced Persistent Threat 1, a unit of the People's Liberation Army operating from a 12-story building in the suburbs of Shanghai that had hundreds, possibly thousands, of staff and the direct support of the Chinese government.[12]

The newest form of mass surveillance in China is the Social Credit System, where citizens and businesses are given or deducted good behavior points depending on their choices.

East Germany

Before the Digital Revolution, one of the world's biggest mass surveillance operations was carried out by the Stasi, the secret police of the former East Germany. By the time the state collapsed in 1989, the Stasi had built up an estimated civilian network of 300,000 informants (approximately one in fifty of the population), who monitored even minute hints of political dissent among other citizens. Many West Germans visiting friends and family in East Germany were also subject to Stasi spying, as well as many high-ranking West German politicians and persons in the public eye.

Most East German citizens were well aware that their government was spying on them, which led to a culture of mistrust: touchy political issues were only discussed in the comfort of their own four walls and only with the closest of friends and family members, while widely maintaining a façade of unquestioning followership in public.

European Union

The right to privacy is a highly developed area of law in Europe. The Data Protection Directive regulates the processing of personal data within the European Union. For comparison, the US has no data protection law that is comparable to this; instead, the US regulates data protection on a sectoral basis.[15]

Since early 2012, the European Union has been working on a General Data Protection Regulation to replace the Data Protection Directive and harmonise data protection and privacy law. On 20 October 2013, a committee at the European Parliament backed the measure, which, if it is enacted, could require American companies to seek clearance from European officials before complying with United States warrants seeking private data. The vote is part of efforts in Europe to shield citizens from online surveillance in the wake of revelations about a far-reaching spying program by the U.S. National Security Agency.[16] European Union justice and rights commissioner Viviane Reding said "The question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security." The EU is also asking the US for changes to US legislation to match the legal redress offered in Europe; American citizens in Europe can go to the courts if they feel their rights are infringed but Europeans without right of residence in America cannot.[17] When the EU / US arrangement to implement International Safe Harbor Privacy Principles were struck down by the European Court of Justice, a new framework for transatlantic data flows, called the "EU-US Privacy Shield", was adopted in July 2016.[18][19]

In April 2014, the European Court of Justice declared invalid the EU Data Retention Directive. The Court said it violates two basic rights - respect for private life and protection of personal data.[20] The legislative body of the European Union passed the Data Retention Directive on 15 December 2005. It requires that telecommunication operators retain metadata for telephone, Internet, and other telecommunication services for periods of not less than six months and not more than two years from the date of the communication as determined by each EU member state and, upon request, to make the data available to various governmental bodies. Access to this information is not limited to investigation of serious crimes, nor is a warrant required for access.[21][22]

Undertaken under the *Seventh Framework Programme for research and technological development* (FP7 - Science in Society[23]) some multidisciplinary and mission oriented mass surveillance activities (for example INDECT and HIDE (http://cordis.europa.eu/project/rcn/88614_en.html)) were funded by the European Commission[24] in association with industrial partners.[25][26][27][28]

The INDECT Project ("Intelligent information system supporting observation, searching and detection for security of citizens in urban environment")[29] develops an intelligent urban environment observation system to register and exchange operational data for the automatic detection, recognition and intelligent processing of all information of abnormal behaviour or violence.[30][31]

The main expected results of the INDECT project are:

- Trial of intelligent analysis of video and audio data for threat detection in urban environments,
- Creation of tools and technology for privacy and data protection during storage and transmission of information using quantum cryptography and new methods of digital watermarking,
- Performing computer-aided detection of threats and targeted crimes in Internet resources with privacy-protecting solutions,
- Construction of a search engine for rapid semantic search based on watermarking of content related to child pornography and human organ trafficking,
- Implementation of a distributed computer system that is capable of effective intelligent processing.

HIDE ("Homeland Security, Biometric Identification & Personal Detection Ethics")[32] was a research project funded by the European Commission within the scope of the Seventh RTD Framework Programme (FP7). The consortium, coordinated by Emilio Mordini (http://www.emiliomordini.info),[33] explored the ethical and privacy implications of biometrics and personal detection technologies, focusing on the continuum between personal detection, authentication, identification and mass surveillance.[34]

France

Germany

In 2002 German citizens were tipped off about wiretapping when a software error led to a phone number allocated to the German Secret Service being listed on mobile telephone bills.[35]

India

The Indian parliament passed the Information Technology Act of 2008 with no debate, giving the government fiat power to tap all communications without a court order or a warrant. Section 69 of the act states "Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence."

India is setting up a national intelligence grid called NATGRID,[36] which would be fully set up by May 2011 where each individual's data ranging from land records, Internet logs, air and rail PNR, phone records, gun records, driving license, property records, insurance, and income tax records would be available in real time and with no oversight.[37] With a UID from the Unique Identification Authority of India being given to every Indian from February 2011, the government would be able track people in real time. A national population registry of all citizens will be established by the 2011 census, during which fingerprints and iris scans would be taken along with GPS records of each household.[38][39]

As per the initial plan, access to the combined data will be given to 11 agencies, including the Research and Analysis Wing, the Intelligence Bureau, the Enforcement Directorate, the National Investigation Agency, the Central Bureau of Investigation, the Directorate of Revenue Intelligence and the Narcotics Control Bureau.

Several states within India have already installed CCTV surveillance systems with face matching capabilities using biometrics in Aadhaar.[40] Andhra Pradesh and Telangana are using information linked with Aadhaar across different agencies to create a 360-degree profile of a person, calling it the Integration Information Hub. Other states are now planning to follow this model.[41]

Iran

Iran is one of the five countries on Reporters Without Borders' March 2013 list of "State Enemies of the Internet", countries whose governments are involved in naturally active efforts to news providers . The government runs or controls almost all of the country's institutions for regulating, managing or legislating on telecommunications. The Supreme Council for Cyberspace, which was headed by President Ahmadinejad, was established in March 2012 and now determines digital policy. The construction of a parallel "Iranian Internet", with a high connection speed but fully monitored and censored, is almost complete.[12]

The tools used by the Iranian authorities to monitor and control the Internet include data interception tools capable of Deep Packet Inspection. Interception products from leading Chinese companies such as ZTE and Huawei are in use. The products provided by Huawei to Mobin Net, the leading national provider of mobile broadband, can be used to analyze email content, track browsing history and block access to sites. The products that ZTA sold to the Telecommunication Company of Iran (TCI) offer similar services plus the possibility of monitoring the mobile network. European companies are the source of other spying and data analysis tools. Products designed by Ericsson and Nokia Siemens Networks (later Trovicor) are in use. These companies sold SMS interception and user location products to Mobile Communication Company of Iran and Irancell, Iran's two biggest mobile phone companies, in 2009 and they were used to identify Iranian citizens during the post-election uprising in 2009. The use of Israeli surveillance devices has also been detected in Iran. The network traffic management and surveillance device NetEnforcer was provided by Israel to Denmark and then resold to Iran. Similarly, US equipment has found its way to Iran via the Chinese company ZTE.[12]

Malaysia

In July 2018, the Malaysian police announced the creation of the Malaysian Internet Crime Against Children Investigation Unit (Micac) that is equipped with real-time mass internet surveillance software developed in the United States and is tasked with the monitoring of all Malaysian internet users, with a focus on pornography and child pornography. The system creates a "data library" of users which includes details such as IP addresses, websites, locations, duration and frequency of use and files uploaded and downloaded.[42][43][44]

Mexico

After struggling with drug trafficking and criminal groups for decades Mexico has been strengthening their military mass surveillance. Approximately half of the population in Mexico does not support democracy as a form of government, and believe an authoritarian system is better if social matters are solved through it.[45] The relevance of these political beliefs may make it easier for mass surveillance to take spread within the country. "This does not necessarily mean the end of democratic institutions as a whole—such as free elections or the permanence of critical mass media—but it means strengthening the mechanisms for exercising power that exclude dialogue, transparency and social agreement."[46] Developing intelligence agencies has been on Mexico's radar for a while for means of security.

Netherlands

According to a 2004 report, the government of the Netherlands carries out more clandestine wire-taps and intercepts than any country, per capita, in the world.[47] The Dutch military intelligence service MIVD operates a satellite ground station to intercept foreign satellite links and also a facility to eavesdrop on foreign high-frequency radio traffic.

North Korea

Having attained the nickname ‘surveillance state’, North Korea's government has complete control over all forms of telecommunications and Internet. It is routine to be sent to a prison camp for communicating with the outside world. The government enforces restrictions around the types of appliances North Koreans may own in their home, in case radio or TV sets pick up signals from nearby South Korea, China and Russia.[48] There is no attempt to mask the way this government actively spies on their citizens. In North Korea, an increasing number of citizens do have smartphones. However, these devices are heavily controlled and are being used to censor and observe everything North Koreans do on their phones. Reuters reported in 2015 that Koryolink, North Korea's official mobile phone network, has around 3 million subscribers in a country of 24 million. Obviously, in order to have digital data to draw from, the citizens must have access to phones and other things online.

Russia

The SORM (and SORM-2) laws enable complete monitoring of any communication, electronic or traditional, by eight state agencies, without warrant. These laws seem to be in conflict with Article 23 of the Constitution of Russia which states:[49]

> 1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.
> 2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision.

In 2015, the European Court for Human Rights ruled that the legislation violated Article 8 of the European Convention on Human Rights (*Zakharov v. Russia*).

Yarovaya Law required storage and unconditional access to private communication data for law enforcement.[50]

Singapore

Singapore is known as a city of sensors. Singapore's surveillance structure spreads widely from Closed-circuit television in public areas even around the neighbourhood, internet monitoring/ traffic monitoring and to the use of surveillance metadata for government initiatives. In Singapore, SIM card registration is mandatory even for prepaid card. Singapore's government have the rights to access communication data. Singapore's largest telecompany, Singtel, has close relations to the government and Singapore's laws are broadly phrased to allow the government to obtain sensitive data such as text-messages, email, call logs and web surfing history from its people without the need for court permission.[51]

The installation of mass surveillance cameras in Singapore is an effort to act as a deterrence not only for terror attacks[52] but also for public security such as loan sharks, illegal parking and more.[53] As part of Singapore's Smart Nation initiative to build a network of sensors to collect and connect data from city life (including the citizen's movement), the Singapore government rolled out 1000 sensors ranging from computer chips to surveillance cameras,[54] to track almost everything in Singapore from air quality to public safety in 2014.[55]

In 2016, in a bid to increase security, the Singapore Police Force installed 62,000 police cameras in 10,000 Housing and Development Board (HDB) blocks covering the lifts and multi-storey car parks.[56] With rising security concerns, the number of CCTV cameras in public areas such as monitoring of the public transport system and commercial/ government buildings in Singapore is set to increase.[52]

In 2018, the Singapore government would be rolling out new and more advanced surveillance systems. Starting with Singapore's maritime borders, new panoramic electro-optic sensors will be put in place on the north and south coasts, monitoring a 360-degree view of the area.[57] A tethered unmanned aerial vehicle (UAV) will also be operational, which can be used during search and rescue operations including hostage situations and public order incidents.[58]

Spain

According to a 2017 report by Privacy International, Spain may be part of a group of 21 European countries that is withholding information, also known as data retention.[59] In 2014, many defense lawyers tried to overturn multiple cases that used mass storage as their evidence to convict, according to the European Agency for Fundamental Rights.[60]

Sweden

Prior to 2009, the National Defence Radio Establishment (FRA) was limited to wireless signals intelligence (SIGINT), although it was left largely unregulated.[61] In December 2009, new legislation went into effect, allowing the FRA to monitor cable bound signals passing the Swedish border.[62] Communications service providers are legally required, under confidentiality, to transfer cable communications crossing Swedish borders to specific "interaction points", where data may be accessed after a court order.[63]

The FRA has been contested since the change in its legislation, mainly because of the public perception the change would enable mass surveillance.[64] The FRA categorically deny this allegation,[62][65] as they are not allowed to initialize any surveillance on their own,[66] and has no direct access to communication lines.[67] All SIGINT has to be authorized by a special court and meet a set of narrow requirements, something Minister for Defence Sten Tolgfors have been quoted as saying, "should render the debate on mass surveillance invalid."[68][69][70] Due to the architecture of Internet backbones in the Nordic area, a large portion of Norwegian and Finnish traffic will also be affected by the Swedish wiretapping.

Syria

Syria is one of the five countries on Reporters Without Borders' March 2013 list of "State Enemies of the Internet", countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. Syria has stepped up its web censorship and cyber-monitoring as the country's civil war has intensified. At least 13 Blue Coat proxy servers are in use, Skype calls are intercepted, and social engineering techniques, phishing, and malware attacks are all in use.[12]

Turkey

The failed coup attempt June 15, 2016 led to an authoritarian shift that uses mass surveillance to suppress opposite views. Digital surveillance is part of everyday life due to the box the government puts the Turkish citizens in. It is increasingly difficult to release any academic knowledge beyond what the Turkish government wants to be released. They have a digital and physical strong hold over any knowledge that goes against their regime. Today, the surveillance of academicians goes along with the state's oppression in Turkey. It is hard to say what will happen in the next few years in Turkey as they become increasingly more authoritarian. The centralization of state power along with digitalization expands the scope of the state surveillance. The digitalization and the centralization of state power are closely related to the regime of power that becomes prominent in this conjuncture.[71] National security and terrorism are Turkey's main explanations to the world on this topic, although there is clearly more happening there. According to the report of Human Rights Joint Platform published on February 23, 2017, during the nine months period of the state of emergency, the number of dismissed academicians reached 4,811, increasing to 7,619 with the addition of academicians who were working in the universities closed after the failed coup attempt.[71] The extended surveillance in Turkey helped them to control the population at a massive scale.

United Kingdom

State surveillance in the United Kingdom has formed part of the public consciousness since the 19th century. The postal espionage crisis of 1844 sparked the first panic over the privacy of citizens.[72] However, in the 20th century, electronic surveillance capabilities grew out of wartime signal intelligence and pioneering code breaking.[73] In 1946, the Government Communications Headquarters (GCHQ) was formed. The United Kingdom and the United States signed the bilateral UKUSA Agreement in 1948. It was later broadened to include Canada, Australia and New Zealand, as well as cooperation with several "third-party" nations. This became the cornerstone of Western intelligence gathering and the "Special Relationship" between the UK and the USA.[74]

After the growth of the Internet and development of the World Wide Web, a series of media reports in 2013 revealed more recent programs and techniques involving GCHQ, such as Tempora.[75]

The use of these capabilities is controlled by laws made in the UK Parliament. In particular, access to the content of private messages (that is, interception of a communication) must be authorized by a warrant signed by a Secretary of State.[76][77][78] In addition European Union data privacy law applies in UK law. The UK exhibits governance and safeguards as well as use of electronic surveillance.[79][80][81]

The Investigatory Powers Tribunal, a judicial oversight body for the intelligence agencies, ruled in December 2014 that the legislative framework in the United Kingdom does not breach the European Convention on Human Rights.[82][83][84] However, the Tribunal stated in February 2015 that one particular aspect, the data-sharing arrangement that allowed UK Intelligence services to request data from the US surveillance programs Prism and Upstream, had been in contravention of human rights law prior to this until two paragraphs of additional information, providing details about the procedures and safeguards, were disclosed to the public in December 2014.[85][86][87]

In its December 2014 ruling, the Investigatory Powers Tribunal found that the legislative framework in the United Kingdom does not permit mass surveillance and that while GCHQ collects and analyses data in bulk, it does not practice mass surveillance.[82][83][84] A report on Privacy and Security published by the Intelligence and Security Committee of Parliament also came to this view, although it found past shortcomings in oversight and said the legal

framework should be simplified to improve transparency.[88][89][90] This view is supported by independent reports from the Interception of Communications Commissioner.[91] However, notable civil liberties groups continue to express strong views to the contrary and plan to appeal the ruling to the European Court of Human Rights,[92] while others have criticised these viewpoints in turn.[93]

The Regulation of Investigatory Powers Act 2000 (RIP or RIPA) is a significant piece of legislation that granted and regulated the powers of public bodies to carry out surveillance and investigation.[94] In 2002 the UK government announced plans to extend the Regulation of Investigatory Powers Act so that at least 28 government departments would be given powers to access metadata about citizens' web, e-mail, telephone and fax records, without a warrant and without a subject's knowledge.[95]

RAF Menwith Hill, a large site in the United Kingdom, part of ECHELON and the UKUSA Agreement

The Protection of Freedoms Act 2012 includes several provisions related to controlling and restricting the collection, storage, retention, and use of information in government databases.[96]

Supported by all three major political parties, the UK Parliament passed the Data Retention and Investigatory Powers Act in July 2014 to ensure police and security services retain existing powers to access phone and Internet records.[97][98]

This was superseded by the Investigatory Powers Act 2016, a comprehensive statute which made public a number of previously secret powers (equipment interference, bulk retention of metadata, intelligence agency use of bulk personal datasets), and enables the Government to require internet service providers and mobile phone companies to maintain records of (but not the content of) customers' Internet connections for 12 months. In addition, it created new safeguards, including a requirement for judges to approve the warrants authorised by a Secretary of State before they come into force.[99][100] The Act was informed by two reports by David Anderson QC, the UK's Independent Reviewer of Terrorism Legislation: A Question of Trust (2015)[101] and the report of his Bulk Powers Review (2016),[102] which contains a detailed appraisal (with 60 case studies) of the operational case for the powers often characterised as mass surveillance. It may yet require amendment as a consequence of legal cases brought before the Court of Justice of the European Union[103] and the European Court of Human Rights.[104]

Many advanced nation-states have implemented laws that partially protect citizens from unwarranted intrusion, such as the Human Rights Act 1998 and Data Protection Act 1998 in the United Kingdom, and laws that require a formal warrant before private data may be gathered by a government.

The UK is a member of the European Union, participates in its programs, and is subject to EU policies and directives on surveillance.

The vast majority of video surveillance cameras in the UK are not operated by government bodies, but by private individuals or companies, especially to monitor the interiors of shops and businesses. According to 2011 Freedom of Information Act requests, the total number of local government operated CCTV cameras was around 52,000 over the entirety of the UK.[105] The prevalence of video surveillance in the UK is often overstated due to unreliable estimates being requoted;[106] for example one report in 2002 extrapolated from a very small sample to estimate the number of cameras in the UK at 4.2 million (of which 500,000 in London).[107] More reliable estimates put the number of private and local government operated cameras in the United Kingdom at around 1.85 million in 2011.[108]

United States

Historically, mass surveillance was used as part of wartime censorship to control communications that could damage the war effort and aid the enemy. For example, during the world wars, every international telegram from or to the United States sent through companies such as Western Union was reviewed by the US military. After the wars were

over, surveillance continued in programs such as the Black Chamber following World War I and project Shamrock following World War II.[109] COINTELPRO projects conducted by the U.S. Federal Bureau of Investigation (FBI) between 1956 and 1971 targeted various "subversive" organizations, including peaceful anti-war and racial equality activists such as Albert Einstein and Martin Luther King Jr.

Billions of dollars per year are spent, by agencies such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), to develop, purchase, implement, and operate systems such as Carnivore, ECHELON, and NarusInsight to intercept and analyze the immense amount of data that traverses the Internet and telephone system every day.[110]

Since the September 11, 2001, terrorist attacks, a vast domestic intelligence apparatus has been built to collect information using the NSA, FBI, local police, state homeland security offices and military criminal investigators. The intelligence apparatus collects, analyzes and stores information about millions of (if not all) American citizens, many of whom have not been accused of any wrongdoing.[111][112]

Under the Mail Isolation Control and Tracking program, the U.S. Postal Service photographs the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces in 2012. The U.S. Postmaster General stated that the system is primarily used for mail sorting, but the images are available for possible use by law enforcement agencies.[113] Created in 2001 following the anthrax attacks that killed five people, it is a sweeping expansion of a 100-year-old program called "mail cover" which targets people suspected of crimes.[114]

The FBI developed the computer programs "Magic Lantern" and CIPAV, which they can remotely install on a computer system, in order to monitor a person's computer activity.[115]

The NSA has been gathering information on financial records, Internet surfing habits, and monitoring e-mails. They have also performed extensive analysis of social networks such as Myspace.[116]

The PRISM special source operation system legally immunized private companies that cooperate voluntarily with U.S. intelligence collection. According to *The Register*, the FISA Amendments Act of 2008 "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant" when one of the parties is outside the U.S.[117] PRISM was first publicly revealed on 6 June 2013, after classified documents about the program were leaked to *The Washington Post* and *The Guardian* by American Edward Snowden.

The Communications Assistance for Law Enforcement Act (CALEA) requires that all U.S. telecommunications and Internet service providers modify their networks to allow easy wiretapping of telephone, VoIP, and broadband Internet traffic.[118][119][120]

In early 2006, *USA Today* reported that several major telephone companies were providing the telephone call records of U.S. citizens to the National Security Agency (NSA), which is storing them in a large database known as the NSA call database. This report came on the heels of allegations that the U.S. government had been conducting electronic surveillance of domestic telephone calls without warrants.[121] In 2013, the existence of the Hemisphere Project, through which AT&T provides telephone call data to federal agencies, became publicly known.

Traffic cameras, which were meant to help enforce traffic laws at intersections, may be used by law enforcement agencies for purposes unrelated to traffic violations.[122] Some cameras allow for the identification of individuals inside a vehicle and license plate data to be collected and time stamped for cross reference with other data used by police.[123] The Department of Homeland Security is funding networks of surveillance cameras in cities and towns as part of its efforts to combat terrorism.[124]

The New York City Police Department infiltrated and compiled dossiers on protest groups before the 2004 Republican National Convention, leading to over 1,800 arrests.[125]

Modern surveillance in the United States was thought of more of a wartime effort before Snowden disclosed in depth information about the National Security Agency in June 2013.[126] The constant development and improvements of the Internet and technology has made it easier for mass surveillance to take hold. Such revelations allow critical commentators to raise questions and scrutinize the implementation, use, and abuse of networking technologies, devices, and software systems that partake in a "global surveillant assemblage" (Bogard 2006; Collier and Ong 2004; Haggerty and Ericson 2000; Murakami Wood 2013).[126] The NSA collected millions of Verizon user's telephone records in between 2013-2014. The NSA also collected data through Google and Facebook with a program called 'Prism'. Journalists through Snowden published nearly 7,000 top-secret documents since then, yet the information disclosed seems to be less than 1% of the entire information. Having access to every individual's private records seems to directly contradict the fourth amendment.

Vietnam

Vietnam is one of the five countries on Reporters Without Borders' March 2013 list of "State Enemies of the Internet", countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. Most of the country's 16 service providers are directly or indirectly controlled by the Vietnamese Communist Party. The industry leader, Vietnam Posts and Telecommunications Group, which controls 74 per cent of the market, is state-owned. So is Viettel, an enterprise of the Vietnamese armed forces. FPT Telecom is a private firm, but is accountable to the Party and depends on the market leaders for bandwidth.[12]

Service providers are the major instruments of control and surveillance. Bloggers monitored by the government frequently undergo man-in-the-middle attacks. These are designed to intercept data meant to be sent to secure (https) sites, allowing passwords and other communication to be intercepted.[12] According to a July 2012 Freedom House report, 91 percent of survey respondents connected to the Internet on their mobile devices and the government monitors conversations and tracks the calls of "activists" or "reactionaries."[127]

Commercial mass surveillance

As a result of the digital revolution, many aspects of life are now captured and stored in digital form. Concern has been expressed that governments may use this information to conduct mass surveillance on their populations. Commercial mass surveillance often makes use of copyright laws and "user agreements" to obtain (typically uninformed) 'consent' to surveillance from consumers who use their software or other related materials. This allows gathering of information which would be technically illegal if performed by government agencies. This data is then often shared with government agencies - thereby - in practice - defeating the purpose of such privacy protections.

One of the most common forms of mass surveillance is carried out by commercial organizations. Many people are willing to join supermarket and grocery loyalty card programs, trading their personal information and surveillance of their shopping habits in exchange for a discount on their groceries, although base prices might be increased to encourage participation in the program.

Through programs like Google's AdSense, OpenSocial and their increasing pool of so-called "web gadgets", "social gadgets" and other Google-hosted services many web sites on the Internet are effectively feeding user information about sites visited by the users, and now also their social connections, to Google. Facebook also keep this information, although its acquisition is limited to page views within Facebook. This data is valuable for authorities, advertisers and others interested in profiling users, trends and web site marketing performance. Google, Facebook and others are increasingly becoming more guarded about this data as their reach increases and the data becomes more all inclusive, making it more valuable.[128]

New features like geolocation give an even increased admission of monitoring capabilities to large service providers like Google, where they also are enabled to track one's physical movements while users are using mobile devices, especially those which are syncing without any user interaction. Google's Gmail service is increasingly employing features to work as a stand-alone application which also might activate while a web browser is not even active for synchronizing; a feature mentioned on the Google I/O 2009 developer conference while showing the upcoming HTML5 features which Google and others are actively defining and promoting.[129]

In 2008 at the World Economic Forum in Davos, Google CEO Eric Schmidt, said: "The arrival of a truly mobile Web, offering a new generation of location-based advertising, is set to unleash a 'huge revolution'".[130] At the Mobile World Congress in Barcelona on 16 February 2010, Google presented their vision of a new business model for mobile operators and trying to convince mobile operators to embrace location-based services and advertising. With Google as the advertising provider, it would mean that every mobile operator using their location-based advertising service would be revealing the location of their mobile customers to Google.[131]

> Google will also know more about the customer - because it benefits the customer to tell Google more about them. The more we know about the customer, the better the quality of searches, the better the quality of the apps. The operator one is "required", if you will, and the Google one will be optional. And today I would say, a minority choose to do that, but I think over time a majority will... because of the stored values in the servers and so forth and so on....
>
> — 2010 Mobile World Congress keynote speech, Google CEO Eric Schmidt[132]

Organizations like the Electronic Frontier Foundation are constantly informing users on the importance of privacy, and considerations about technologies like geolocation.

Computer company Microsoft patented in 2011 a product distribution system with a camera or capture device that monitors the viewers that consume the product, allowing the provider to take "remedial action" if the actual viewers do not match the distribution license.[133]

Reporters Without Borders' March 2013 *Special report on Internet Surveillance* contained a list of "Corporate Enemies of the Internet", companies that sell products that are liable to be used by governments to violate human rights and freedom of information. The five companies on the initial list were: Amesys (France), Blue Coat Systems (U.S.), Gamma (UK and Germany), Hacking Team (Italy), and Trovicor (Germany), but the list was not exhaustive and is likely to be expanded in the future.[12]

Surveillance state

A surveillance state is a country where the government engages in pervasive surveillance of large numbers of its citizens and visitors. Such widespread surveillance is usually justified as being necessary for national security, such as to prevent crime or acts of terrorism, but may also be used to stifle criticism of and opposition to the government.

Examples of early surveillance states include the former Soviet Union and the former East Germany, which had a large network of informers and an advanced technology base in computing and spy-camera technology.[134] But these states did not have today's technologies for mass surveillance, such as the use of databases and pattern recognition software to cross-correlate information obtained by wire tapping, including speech recognition and telecommunications traffic analysis, monitoring of financial transactions, automatic number plate recognition, the tracking of the position of mobile telephones, and facial recognition systems and the like which recognize people by their appearance, gait, DNA profiling, etc.

Germans protesting against the NSA surveillance program PRISM at Checkpoint Charlie in Berlin

Smart cities

The development of smart cities has seen the increased adoption of surveillance technologies by governments, although the primary purpose of surveillance in such cities is to use information and communication technologies to improve the urban environment. The implementation of such technology by a number of cities has resulted in increased efficiencies in urban infrastructure as well as improved community participation. Sensors and systems monitor a smart city's infrastructure, operations and activities and aim to help it run more efficiently. For example, the city could use less electricity; its traffic run more smoothly with fewer delays; its citizens use the city with more safety; hazards can be dealt with faster; citizen infractions of rules can be prevented, and the city's infrastructure; power distribution and roads with traffic lights for example, dynamically adjusted to respond to differing circumstances.[135]

The development of smart city technology has also led to an increase in potential unwarranted intrusions into privacy and restrictions upon autonomy. The widespread incorporation of information and communication technologies within the daily life of urban residents results in increases in the surveillance capacity of states - to the extent that individuals may be unaware of what information is being accessed, when the access occurs and for what purpose. It is possible that such conditions could give rise to the development of an electronic police state. Shanghai, Amsterdam, San Jose, Dubai, Barcelona, Madrid, Stockholm, and New York are all cities that use various techniques from smart city technology.

Electronic police state

An electronic police state is a state in which the government aggressively uses electronic technologies to record, collect, store, organize, analyze, search, and distribute information about its citizens.[136][137] Electronic police states also engage in mass government surveillance of landline and cellular telephone traffic, mail, email, web surfing, Internet searches, radio, and other forms of electronic communication as well as widespread use of video surveillance. The information is usually collected in secret.

Banner in Bangkok, observed on 30 June 2014 during the 2014 Thai coup d'état, informing the Thai public that 'like' or 'share' activity on social media could land them in prison

The crucial elements are not politically based, so long as the government can afford the technology and the populace will permit it to be used, an electronic police state can form. The continual use of electronic mass surveillance can result in constant low-level fear within the population, which can lead to self-censorship and exerts a powerful coercive force upon the populace.[138]

Seventeen factors for judging the development of an electronic police state were suggested in *The Electronic Police State: 2008 National Rankings*:[137]

- **Daily documents**: Requirement for the use and tracking of state-issued identity documents and registration.
- **Border and travel control**: Inspections at borders, searching computers and cell phones, demanding decryption of data, and tracking travel within as well as to and from a country.
- **Financial tracking**: A state's ability to record and search financial transactions: checks, credit cards, wires, etc.
- **Gag orders**: Restrictions on and criminal penalties for the disclosure of the existence of state surveillance programs.
- **Anti-crypto laws**: Outlawing or restricting cryptography and/or privacy enhancing technologies.

- **Lack of constitutional protections**: A lack of constitutional privacy protections or the routine overriding of such protections.
- **Data storage**: The ability of the state to store the data gathered.
- **Data search**: The ability to organize and search the data gathered.
- **Data retention requirements**: Laws that require Internet and other service providers to save detailed records of their customers' Internet usage for a minimum period of time.
  - **Telephone data retention requirements**: Laws that require telephone companies to record and save records of their customers' telephone usage.
  - **Cell phone data retention requirements**: Laws that require cellular telephone companies to record and save records of their customers' usage and location.
- **Medical records**: Government access to the records of medical service providers.
- **Enforcement**: The state's ability to use force to seize anyone they want, whenever they want.
- **Lack of *habeas corpus***: Lack of a right for a person under arrest to be brought before a judge or into court in a timely fashion or the overriding of such rights.
- **Lack of a police-intel barrier**: The lack of a barrier between police organizations and intelligence organizations, or the overriding of such barriers.
- **Covert hacking**: State operatives collecting, removing, or adding digital evidence to/from private computers without permission or the knowledge of the computers' owners.
- **Loose or no warrants**: Arrests or searches made without warrants or without careful examination and review of police statements and justifications by a truly independent judge or other third-party.

The list includes factors that apply to other forms of police states, such as the use of identity documents and police enforcement, but go considerably beyond them and emphasize the use of technology to gather and process the information collected.

In popular culture

The concept of being monitored by our government collects a large audience of curious citizens. Mass surveillance has been prominently featured in a wide array of books, films, and other media. Advances in technology over the last century have led to possible social control through the Internet and the conditions of late capitalism. Many directors and writers have been enthralled with the potential stories that could come from mass surveillance. Perhaps the most iconic example of fictional mass surveillance is George Orwell's 1949 novel *Nineteen Eighty-Four*, which depicts a dystopian surveillance state.

Here are a few other works that focus on mass surveillance:

- *We* , a 1920 novel by Russian author Yevgeny Zamyatin , that predates *Nineteen Eighty-Four* and was read by its author George Orwell.
- *Little Brother* is a novel by Cory Doctorow, and is set in San Francisco after a major terrorist attack. The DHS uses technologies such as RFIDs and surveillance cameras to create a totalitarian system of control.
- *The Lives of Others*, is a 2006 German drama film, which movingly conveys the impact that relentless surveillance has on the emotional well-being and the outcome of individuals subjected to it.
- *The Hunger Games* by Suzanne Collins is a trilogy in which 'the capital' has totalitarian surveillance & control over all aspects of the other 'districts'.
- *Digital Fortress*, novel by Dan Brown, involving an NSA code breaking machine called 'TRANSLTR'. The machine read and decrypted email messages, with which the NSA used to foil terrorist attacks and mass murders.

See also

- 2013 global surveillance disclosures
- Broken windows theory, a controversial theory that maintaining and monitoring urban environments in a well-ordered condition may stop further vandalism and escalation into more serious crime.
- Closed-circuit television (CCTV)
- Computer and network surveillance
- Data privacy
- Data retention
- *Discipline and Punish: The Birth of the Prison*, a 1975 book by the French philosopher Michel Foucault.

- Fear § Manipulation
- Global surveillance
- Government databases
- Lawful interception
- List of government surveillance projects
- National security
- Network analysis
- Nothing to hide argument
- Pen register, originally an electronic device that records numbers (but not the audio) called from a particular telephone line, more recently any device or program that performs this function for electronic mail, other digital communications, and particularly communications over the Internet.
- Phone surveillance
- Police state
- Radio-frequency identification (RFID), the wireless identification and tracking of tags attached to objects.
- Right to privacy
- Security culture
- Signals intelligence (SIGINT)
- Sousveillance, the recording of an activity by a participant in the activity, cameras (or other sensors) affixed to property, or surveillance done by non-authorities.
- Surveillance capitalism
- Telephone tapping in the Eastern Bloc
- Tracking system
- Traffic analysis

References

1. "Mass Surveillance" (https://www.privacyinternational.org/node/52). Privacy International. Retrieved 20 April 2017.
2. TATLOW, DIDI KIRSTEN (2013-06-28), *U.S. Prism, Meet China\u2019s Golden Shield* (http://rendezvous.blogs.nytimes.com/2013/06/28/u-s-prism-meet-chinas-golden-shield/), "[...] a Beijing lawyer named Xie Yanyi filed a public information request with the police asking about China's own surveillance operations. [...] 'Most people were critical about the U.S. and supported Snowden.' [he said...] Then the discussion started shifting to take in China's own surveillance issues."
3. Mark Hosenball and John Whitesides (2013-06-07). "Reports on surveillance of Americans fuel debate over privacy, security" (https://www.reuters.com/article/2013/06/07/us-usa-wiretaps-verizon-idUSBRE95502920130607). *Reuters*. Retrieved 17 December 2013.
4. Kuehn, Kathleen (2016-12-09). *The Post-Snowden Era: Mass Surveillance and Privacy in New Zealand* (https://books.google.com/books?id=JP6lDQAAQBAJ&pg=PA47). Bridget Williams Books. ISBN 9780908321087. Retrieved 8 January 2017.
5. "Snowden: Mass Surveillance Needs Global Solution" (https://en.tempo.co/read/news/2013/11/04/074526933/Snowden-Mass-Surveillance-Needs-Global-Solution). Retrieved 8 January 2017.
6. Lyon, David (2015-10-19). *Surveillance After Snowden* (https://books.google.com/books?id=gBbICgAAQBAJ&pg=PT46). John Wiley & Sons. ISBN 9780745690889. Retrieved 8 January 2017.
7. "Towards a world without mass surveillance" (https://internetnz.nz/sites/default/files/submissions/Towards_a_world_without_mass_surveillance.pdf) (PDF). Retrieved 8 January 2017.
8. "Surveillance Monitor 2007 - International country rankings" (https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings). Privacy International. 28 December 2007.
9. Tom Steinert-Threlkeld (13 August 2008). "Police Surveillance: Go Snoop, Yourself" (http://blogs.zdnet.com/BTL/?p=9662). ZDNet.
10. "YouGov / Daily Telegraph Survey Results" (http://www.yougov.co.uk/extranets/ygarchives/content/pdf/TEL060101024_3.pdf) (PDF). YouGov. 2006. Retrieved 15 September 2013.
11. "Why a Surveillance Society Clock?" (https://www.aclu.org/technology-and-liberty/why-surveillance-society-clock). American Civil Liberties Union. 4 September 2007. Retrieved 15 September 2013.

12. *The Enemies of the Internet Special Edition : Surveillance* (http://surveillance.rsf.org/en/) Archived (https://web.archive.org/web/20130831072750/http://surveillance.rsf.org/en/) 31 August 2013 at the Wayback Machine, Reporters Without Borders, 12 March 2013
13. ONI Asia (http://www.oni-asia.net/), web site, OpenNet Initiative, retrieved 15 September 2013.
14. "Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform" (http://www.nartv.org/mirror/breachingtrust.pdf), Nart Villeneuve, Information Warfare Monitor and ONI Asia, 1 October 2008.
15. See Julia M. Fromholz, The European Union Data Privacy Directive, 15 Berkeley Tech. L.J. 471, 472 (2000); Dean William Harvey & Amy White, The Impact of Computer Security Regulation on American Companies, 8 Tex. Wesleyan L. Rev. 505 (2002); Kamaal Zaidi, Harmonizing U.S.-EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data, 12 Mich.St. J. Int'l L. 169 (2003).
16. "Rules Shielding Online Data From N.S.A. and Other Prying Eyes Advance in Europe" (https://www.nytimes.com/2013/10/22/business/international/eu-panel-backs-plan-to-shield-online-data.html), James Kanter and Mike Scott, *New York Times*, 21 October 2013. Retrieved 22 October 2013.
17. Traynor, Ian (26 November 2013). "NSA surveillance: Europe threatens to freeze US data-sharing arrangements" (https://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing). *The Guardian*. Retrieved 1 December 2013.
18. "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" (http://europa.eu/rapid/press-release_IP-16-216_en.htm) (Press release). European Commission. 2 February 2016. Retrieved 24 February 2016; "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield" (http://europa.eu/rapid/press-release_IP-16-433_en.htm) (Press release). European Commission. 29 February 2016. Retrieved 7 March 2016; "European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows" (http://europa.eu/rapid/press-release_IP-16-2461_en.htm) (Press release). European Commission. 12 July 2016. Retrieved 16 July 2016.
19. "U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await" (https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=0). *New York Times*. 2 February 2016. Retrieved 24 February 2016; "Privacy Shield deal lets US tech firms transfer European customers' data again" (https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union). *The Guardian*. 8 July 2016. Retrieved 8 July 2016; "Privacy Shield forced US to be 'transparent' about intelligence agencies" (http://www.euractiv.com/section/digital/news/privacy-shield-forced-us-to-be-transparent-about-intelligence-agencies/). *EurActiv*. 12 July 2016. Retrieved 16 July 2016.
20. "Top EU court rejects EU-wide data retention law" (https://www.bbc.co.uk/news/world-europe-26935096). BBC. 8 April 2014. Retrieved 7 September 2014.
21. "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC" (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF), L 105/54, *Official Journal of the European Union*, 13 April 2006. Retrieved 20 September 2013.
22. "Joint letter to Cecilia Malmström, European Commissioner for Home Affairs, from Dr. Patrick Breyer and 105 additional parties" (http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf), 22 June 2010.
23. "FP7 - Science in Society" (http://cordis.europa.eu/search/index.cfm?fuseaction=prog.document&PG_RCN=8748316), Community Research and Development Information Service (CORDIS), European Commission, 30 December 2006.
24. "FP7 Security Research" (http://cordis.europa.eu/fp7/security/projects_en.html), Community Research and Development Information Service (CORDIS), European Commission, 3 September 2012. Retrieved 15 September 2013.
25. "The EU Security-Industrial Complex, an interview with Ben Hayes about his book *NeoConOpticon* " (http://www.heise.de/tp/r4/artikel/31/31198/1.html), Matthias Monroy, *Telepolis* (Heise Zeitschriften Verlag), 25 September 2009. Retrieved 15 September 2013.
26. *NeoConOpticon — The EU Security-Industrial Complex* (http://www.statewatch.org/analyses/neoconopticon-report.pdf), Ben Hayes, Transnational Institute (TNI) and Statewatch, 25 September 2009, 84 pages,ISSN 1756-851X (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:1756-851X). Retrieved 15 September 2013.

27. "Totalüberwachung der realen und virtuellen Räume" (http://www.heise.de/tp/r4/artikel/31/31176/1.html) (in German) ("Total control of the real and virtual spaces"), Florian Rötzer, *Telepolis* (Heise Zeitschriften Verlag), 22 September 2009. Retrieved 15 September 2013. (English translation (https://translate.google.com/translate?hl=&sl=auto&tl=en&u=http%3A%2F%2Fwww.heise.de%2Ftp%2Fartikel%2F31%2F31176%2F1.html&sandbox=1))
28. *Towards a more secure society and increased industrial competitiveness: Security Research Projects under the 7th Framework Programme for Research* (ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf), European Commission, May 2009, 100 pages. Retrieved 15 September 2013.
29. INDECT project homepage (http://www.indect-project.eu/), AGH - University of Science and Technology (Poland). Retrieved 17 September 2013.
30. "INDECT: Intelligent information system supporting observation, searching and detection for security of citizens in urban environment" (http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=4&CAT=PROJ&QUERY=011f30e52539:b685:00e1e967&RCN=89374), EU Research Projects, Community Research and Development Information Service (CORDIS), European Commission, 4 September 2013. Retrieved 17 September 2013.
31. "EU funding 'Orwellian' artificial intelligence plan to monitor public for 'abnormal behaviour' " (https://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html), Ian Johnston, *The Telegraph* (UK), 19 September 2009. Retrieved 17 September 2013.
32. HIDE - "HOMELAND SECURITY, BIOMETRIC IDENTIFICATION AND PERSONAL DETECTION ETHICS", Community Research and Development Information Service, http://cordis.europa.eu/project/rcn/88614_en.html. Retrieved July 17, 2016
33. Mordini E. (2008), Nothing to Hide. Biometrics, Privacy and Private Sphere, in Schouten B. et al. (eds.): BIOID 2008, Biometrics and Identity Management, LNCS 5372, Springer-Verlag Berlin Heidelberg, 247–257. https://link.springer.com/chapter/10.1007/978-3-540-89991-4_27. Retrieved July, 17; 2016.
34. HIDE Project Overview, http://www.cssc.eu/public/FINAL%20BROCHURE.pdf. Retrieved July 17, 2016
35. Tim Richardson (4 November 2002). "German secret service taps phones, bills buggees" (https://www.theregister.co.uk/2002/11/04/german_secret_service_taps_phones/). *The Register*. Retrieved 27 January 2011.
36. "Centralised System to Monitor Communications" (http://pib.nic.in/release/release.asp?relid=54679), reply by Shri Gurudas Kamat, Minister of State for Communications and Information Technology in Rajya Sabha, Press Information Bureau, 26 November 2009. Retrieved 17 September 2013.
37. Mohan, Vishwa (2 October 2009). "MHA to make security data tamper-free" (http://timesofindia.indiatimes.com/india/MHA-to-make-security-data-tamper-free/articleshow/5078546.cms). *The Times Of India*. TNN. Retrieved 17 September 2013.
38. India to prepare NPR with 2011 Census (http://www.igovernment.in/site/india-to-prepare-npr-with-2011-census/) Archived (https://web.archive.org/web/20120905052217/http://www.igovernment.in/site/india-to-prepare-npr-with-2011-census/) 5 September 2012 at the Wayback Machine, iGovernment (9.9 Mediaworx), 24 April 2008. Retrieved 17 September 2013.
39. "Election Commission to use Census data, GPS to track voters" (http://www.rediff.com/news/2008/aug/25ec.htm), Rediff (Delhi), 25 August 2008. Retrieved 17 September 2012.
40. "Picture Intelligence Unit – Aadhaar Based Surveillance By Foreign Firms" (https://web.archive.org/web/20180202190150/http://tunein23.com/EN/?p=2757). Archived from the original (http://tunein23.com/EN/?p=2757) on 2018-02-02.
41. "Right to privacy: Data shows states using Aadhaar to build profiles of citizens" (https://www.hindustantimes.com/india-news/despite-govt-denials-states-building-databases-for-360-degree-profiles-of-citizens/story-qnSLHGyZIXiZiO4ce84UuO.html). 2017-08-25.
42. "Watching porn? Cops now have their eyes on you | Malay Mail" (https://www.malaymail.com/s/1650214/watching-porn-cops-now-have-their-eyes-on-you).
43. https://www.nst.com.my/news/exclusive/2018/07/388926/exclusive-police-will-know-if-you-watch-porn
44. "Respect privacy and no to monitoring of internet usage or activity in Malaysia, say ASEAN NGOs" (https://www.theonlinecitizen.com/2018/07/20/respect-privacy-and-no-to-monitoring-of-internet-usage-or-activity-in-malaysia-say-asean-ngos/). 2018-07-20.
45. Arteaga, Nelson. 2017. Mexico: Internal security, surveillance, and authoritarianism. Surveillance & Society 15(3/4): 491-495.

46. Arteaga, Nelson. 2017. Mexico: Internal security, surveillance, and authoritarianism. Surveillance & Society 15(3/4): 491-495.(Artega, 494)
47. "Italy and the Netherlands top wiretap chart" (https://edri.org/edrigramnumber2-14wiretap/), Digital Civil Rights in Europe, EDRI-gram Number 2.14, 15 July 2004. Retrieved 17 September 2013.
48. "North Korea, the surveillance state" (https://www.amnesty.org.uk/north-korea-surveillance-state-prison-camp-internet-phone-technology).
49. "Chapter 2. Rights and Freedoms of Man And Citizen" (http://www.constitution.ru/en/10003000-03.htm), *Constitution of Russia*. Retrieved 17 September 2013.
50. "Draconian Law Rammed Through Russian Parliament" (https://www.hrw.org/news/2016/06/23/draconian-law-rammed-through-russian-parliament). 2016-06-23. Retrieved 2016-08-10.
51. "Tech in Asia - Connecting Asia's startup ecosystem" (https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind).
52. "More surveillance cameras as deterrent" (http://www.straitstimes.com/singapore/more-surveillance-cameras-as-deterrent). 2016-03-18.
53. "Network of CCTV cameras proving effective" (http://www.straitstimes.com/singapore/network-of-cctv-cameras-proving-effective). 2016-03-08.
54. "Seeking Privacy in a City of Sensors" (https://www.citylab.com/life/2017/04/singapore-city-of-sensors/523392/).
55. "1,000 sensors to be rolled out in Singapore as part of 'smart nation' plan" (http://www.straitstimes.com/singapore/1000-sensors-to-be-rolled-out-in-singapore-as-part-of-smart-nation-plan). 2014-10-10.
56. "Installation of 62,000 police cameras in 10,000 HDB blocks, multi-storey carparks complete" (http://www.straitstimes.com/singapore/installation-of-62000-police-cameras-in-10000-hdb-blocks-multi-storey-carparks-complete). 2016-07-11.
57. "Bevy of cameras, high-tech sensors to secure shoreline" (http://www.straitstimes.com/singapore/bevy-of-cameras-high-tech-sensors-to-secure-shoreline). 2016-03-18.
58. "New drones, command vehicles to help police fight crime better" (https://www.channelnewsasia.com/news/singapore/new-drones-command-vehicles-to-help-police-fight-crime-better-9819786).
59. "Report On The National Data Retention Laws Since The CJEU's Tele-2/Watson Judgment" (https://privacyinternational.org/advocacy-briefing/735/report-national-data-retention-laws-cjeus-tele-2watson-judgment). *Privacy International*. September 1, 2017.
60. "Data retention across the EU" (http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention#Slovenia). *European Union Agency for Fundamental Rights*. 2015-12-16. Retrieved 2018-04-29.
61. "SOU 2003:30". p. 154. "Det har således i svensk rätt bedömts att det inte finns något rättsligt skydd för den enskildes integritet mot avlyssning eller inhämtning av signaltrafik som befordras trådlöst" Missing or empty `|url=` (help)
62. Hernadi, Alexandra. "I morgon börjar FRA-lagen gälla" (http://www.svd.se/nyheter/inrikes/i-morgon-borjar-fra-lagen-galla_3868431.svd) (in Swedish). SvD. Retrieved 10 March 2014.
63. "Prop. 2006/07:63" (http://www.regeringen.se/download/2ee1ba0a.pdf?major=1&minor=78367&cn=attachme) (PDF).
64. Bjurbo, Peter. "FRA-spaning inte så stor som framställts" (https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=2184064) (in Swedish). Sveriges Radio. Retrieved 10 March 2014.
65. "FRA Påståenden och klargöranden" (https://web.archive.org/web/20070611040026/http://www.fra.se/omfra_faq_lag.shtml) (in Swedish). FRA. 2009. Archived from the original (http://www.fra.se/omfra_faq_lag.shtml) on 2007-06-11.
66. "Datainspektionens redovisning av regeringsuppdraget Fö2009/355/SUND" (http://www.datainspektionen.se/Documents/beslut/2010-12-07-fra.pdf) (PDF). The Swedish Data Inspection Board. Retrieved 10 March 2014.
67. "SFS 2008:717" (https://lagen.nu/2008:717#P4aS1).
68. Sjögren, Per-Anders. "Alliansen enig om stora ändringar i FRA-lag" (https://web.archive.org/web/20140310123656/http://rod.se/alliansen-enig-om-stora-%C3%A4ndringar-i-fra-lag/) (in Swedish). Riksdag & Departement. Archived from the original (http://rod.se/alliansen-enig-om-stora-%C3%A4ndringar-i-fra-lag/) on 10 March 2014. Retrieved 10 March 2014.
69. Bynert, Simon. "Militärt hot villkor för FRA-spaning" (http://www.svd.se/nyheter/inrikes/militart-hot-villkor-for-fra-spaning_1788753.svd) (in Swedish). SvD. Retrieved 10 March 2014.

70. "Alliansen enig om stärkt integritet, tydligare reglering och förbättrad kontroll i kompletteringar till signalspaningslagen" (https://web.archive.org/web/20140310123055/http://www.regeringen.se/sb/d/10911/a/112332) (in Swedish). Regeringen. Archived from the original (http://www.regeringen.se/sb/d/10911/a/112332) on 10 March 2014. Retrieved 10 March 2014.
71. 2017. State vs. Academy in Turkey: Academy Under Surveillance. Surveillance & Society 15(3/4): 550-556.
72. Vincent, David (1 October 2013). "Surveillance, privacy and history" (http://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history). *History & Policy*. History & Policy. Retrieved 27 July 2016.
73. "How the British and Americans started listening in" (https://www.bbc.co.uk/news/magazine-35491822). *BBC*. 8 February 2016. Retrieved 24 February 2016.
74. Adam White (29 June 2010). "How a Secret Spy Pact Helped Win the Cold War" (http://content.time.com/time/nation/article/0,8599,2000262,00.html). *Time*.
75. "US and Britain team up on mass surveillance" (https://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance). *The Guardian*. 22 June 2013. Retrieved 13 May 2015.
76. "The Andrew Marr Show Interview: Theresa May, MP Home Secretary" (http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/2311201402.pdf) (PDF). BBC. 23 November 2014. Retrieved 6 December 2014. "Well I guess what he's talking about is the fact that for certain aspects and certain of the more intrusive measures that our security service and police have available to them – i.e. Intercept, intercepting people's telephones and some other intrusive measures – the decision is taken by the Secretary of State, predominantly me. A significant part of my job is looking at these warrants and signing these warrants. I think it's ... Some people argue that should be to judges....I think it's very important that actually those decisions are being taken by somebody who is democratically accountable to the public. I think that's an important part of our system. I think it's a strength of our system."
77. "The Law" (http://www.gchq.gov.uk/how_we_work/running_the_business/oversight/Pages/The-law.aspx). GCHQ. Retrieved 17 December 2013.
78. "Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme" (https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf) (PDF). Intelligence and Security Committee of Parliament. 17 July 2013. Retrieved 17 December 2013.
79. "Other safeguards and oversight" (https://web.archive.org/web/20150206141103/http://www.ipt-uk.com/section.aspx?pageid=27). The Investigatory Powers Tribunal. Archived from the original (http://www.ipt-uk.com/section.aspx?pageid=27) on 6 February 2015. Retrieved 6 February 2015.
80. "Intelligence and Security Committee open evidence session" (http://www.parliament.uk/business/news/2013/november-/isc-open-evidence-session/). UK Parliament. 7 November 2013. Retrieved 18 December 2013.; "Spy chiefs public hearing: as it happened" (https://www.telegraph.co.uk/news/uknews/defence/10432629/Spy-chiefs-public-hearing-as-it-happened.html). *The Telegraph*. 7 November 2013. Retrieved 18 December 2013.
81. "Britain's spy chiefs will be questioned in public for the first time, under radical reforms of the way Parliament monitors the intelligence agencies" (https://www.telegraph.co.uk/news/politics/9669262/Top-spooks-to-be-quizzed-in-public.html). *The Telegraph*. 10 November 2012. Retrieved 18 December 2013.
82. "GCHQ does not breach human rights, judges rule" (https://www.bbc.co.uk/news/uk-30345801). BBC. 5 December 2014. Retrieved 6 December 2014.
83. "IPT rejects assertions of mass surveillance" (https://web.archive.org/web/20150206232713/http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/IPT-rejects-assertions-of-mass-surveillance.aspx). GCHQ. 5 December 2014. Archived from the original (http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/IPT-rejects-assertions-of-mass-surveillance.aspx) on 6 February 2015. Retrieved 7 February 2015.
84. "List of judgments" (https://web.archive.org/web/20150206211011/http://www.ipt-uk.com/section.aspx?pageid=8). Investigatory Powers Tribunal. 5 December 2014. Archived from the original (http://www.ipt-uk.com/section.aspx?pageid=8) on 6 February 2015. Retrieved 7 February 2015. "1. A declaration that the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK which have been obtained by US authorities pursuant to Prism and/or Upstream does not contravene Articles 8 or 10 ECHR. 2. A declaration that the regime in respect of interception under ss8(4), 15 and 16 of the Regulation of investigatory Powers Act 2000 does not contravene Articles 8 or 10 ECHR and does not give rise to unlawful discrimination contrary to Article 14, read together with Articles 8 and/or 10 of the ECHR."
85. "IPT Ruling on Interception" (https://web.archive.org/web/20150206205536/http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/IPT-Ruling-on-Interception-Feb-2014.aspx). GCHQ. 6 February 2015. Archived from the original (http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/IPT-Ruling-on-Interception-Feb-2014.aspx) on 6 February 2015. Retrieved 6 February 2015.

86. "GCHQ censured over sharing of internet surveillance data with US" (https://www.bbc.com/news/uk-31164451). BBC. 6 February 2015. Retrieved 6 February 2015.
87. "UK-US surveillance regime was unlawful 'for seven years'" (https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa). The Guardian. 6 February 2015. Retrieved 6 February 2015.
88. "UK surveillance 'lacks transparency', ISC report says" (https://www.bbc.co.uk/news/uk-31845338). BBC. 12 March 2015. Retrieved 14 March 2015.
89. "Privacy and Security: A modern and transparent legal framework" (http://isc.independent.gov.uk/news-archive/12march2015). Intelligence and Security Committee of Parliament. 12 March 2015. Retrieved 14 March 2015.
90. "Intelligence and security committee report: the key findings" (https://www.theguardian.com/world/2015/mar/12/intelligence-security-committee-report-key-findings). The Guardian. 12 March 2015. Retrieved 14 March 2015.
91. "Statement by the Interception of Communications Commissioner's Office (IOCCO) on the publication of the Interception of Communications Commissioner's Report 2014" (http://www.iocco-uk.info/docs/2015%20Press%20Release%20Final.pdf) (PDF). 12 March 2015. Retrieved 14 March 2015; "Report of the Interception of Communications Commissioner" (http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf) (PDF). March 2015. Retrieved 14 March 2015.
92. "UK surveillance laws need total overhaul, says landmark report" (https://www.theguardian.com/us-news/2015/mar/12/uk-surveillance-laws-need-total-overhaul-says-landmark-report-edward-snowden). The Guardian. 12 March 2015. Retrieved 14 March 2015.
93. "Civil liberty campaigners attacked for saying terror attack is "price worth paying" to prevent mass snooping" (https://www.telegraph.co.uk/news/uknews/defence/11468060/Civil-liberty-campaigners-attacked-for-saying-terror-attack-is-price-worth-paying-to-prevent-mass-snooping.html). *The Telegraph*. 12 March 2015. Retrieved 14 November 2015; Carlile, Alex (13 March 2015). "GCHQ doesn't need any lectures from Liberty" (http://www.thetimes.co.uk/tto/opinion/thunderer/article4380539.ece). *The Times*. Retrieved 14 March 2015.
94. "Regulation of Investigatory Powers Act 2000" (http://www.legislation.gov.uk/ukpga/2000/23/introduction), 2000 Chapter 23, UK Government Legislation. Retrieved 28 September 2013.
95. " 'Massive abuse' of privacy feared" (http://news.bbc.co.uk/1/hi/sci/tech/2038036.stm). *BBC News*. 11 June 2002. Retrieved 5 April 2010.
96. "Protection of Freedoms Bill" (https://www.gov.uk/government/publications/protection-of-freedoms-bill), Home Office, 11 February 2011. Retrieved 28 September 2013.
97. "Emergency data law clears Commons" (http://www.bbc.co.uk/democracylive/house-of-commons-28320473). BBC. 16 July 2014. Retrieved 27 September 2014.
98. "Data Retention Bill set to become law" (http://www.bbc.co.uk/democracylive/house-of-lords-28349828). BBC. 17 July 2014. Retrieved 27 September 2014.
99. "Details of UK website visits 'to be stored for year'" (https://www.bbc.co.uk/news/uk-politics-34715872). *BBC*. 4 November 2015. Retrieved 10 November 2015.
100. "Investigatory powers bill: the key points" (https://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points). *The Guardian*. 4 November 2015. Retrieved 10 November 2015.
101. "A question of trust: report of the investigatory powers review - GOV.UK" (https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review). *www.gov.uk*. Retrieved 2017-07-06.
102. "Investigatory Powers Bill: bulk powers review - GOV.UK" (https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review). *www.gov.uk*. Retrieved 2017-07-06.
103. David Anderson (2017-04-11). "CJEU judgment in Watson/Tele2" (https://www.daqc.co.uk/2017/04/11/cjeu-judgment-in-watson/). *David Anderson QC Lawyer London UK*. Retrieved 2017-07-06.
104. "10 Human Rights Organisations v. United Kingdom | Privacy International" (https://www.privacyinternational.org/node/992). *www.privacyinternational.org*. Retrieved 2017-07-06.
105. "The Price of Privacy: How local authorities spent £515m on CCTV in four years" (http://www.bigbrotherwatch.org.uk/files/priceofprivacy/Price_of_privacy_2012.pdf) (PDF). Big Brother Watch. February 2012. Retrieved 4 February 2015.
106. "FactCheck: how many CCTV cameras? - Channel 4 News" (http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167). Channel4.com. Retrieved 2009-05-08.
107. "CCTV in London" (http://www.urbaneye.net/results/ue_wp6.pdf) (PDF). Retrieved 2009-07-22.
108. "How many cameras are there?" (http://www.cctvusergroup.com/art.php?art=94). CCTV User Group. 2008-06-18. Retrieved 2009-05-08.

109. James Bamford (2008), *The Shadow Factory*, Doubleday, ISBN 0-385-52132-4, Chapter 'Shamrock', especially pg. 163.
110. McCullagh, Declan (30 January 2007). "FBI turns to broad new wiretap method" (http://www.zdnet.com/news/fbi-turns-to-broad-new-wiretap-method/151059). *ZDNet News*. Retrieved 2009-03-13.
111. Data Priest and William M. Arkin (20 December 2010). "Monitoring America" (http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/). *Top Secret America, A Washington Post Investigation*. Washington Post. Retrieved 27 January 2011.
112. Mui, Ylan (29 July 2013). "Growing use of FBI screens raises concerns about accuracy, racial bias" (https://www.washingtonpost.com/business/economy/growing-use-of-fbi-screens-raises-concerns-over-accuracy-racial-bias/2013/07/29/d201ecda-f49f-11e2-aa2e-4088616498b4_story.html). *Washington Post*. Retrieved 2 August 2013.
113. "AP Interview: USPS takes photos of all mail" (http://bigstory.ap.org/article/ap-interview-usps-takes-photos-all-mail), Associated Press (AP), 2 August 2013.
114. "U.S. Postal Service Logging All Mail for Law Enforcement" (https://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?pagewanted=all&_r=0), Ron Nixon, *New York Times*, July 3, 2013. Retrieved 25 September 2013.
115. Kevin Poulsen (18 July 2007). "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" (https://www.wired.com/politics/law/news/2007/07/fbi_spyware). *Wired Magazine*. Condé Nast. Retrieved 19 September 2013.
116. "Is the NSA reading your MySpace profile?" (https://archive.is/20120720043006/http://news.com.com/2061-10789_3-6082047.html), Dawn Kawamoto, *CNET News*, 9 June 2006. Retrieved 19 September 2013.
117. Glenn Greenwald (31 July 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'" (https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data). *The Guardian*. Retrieved 2 August 2013.
118. "CALEA Archive" (https://web.archive.org/web/20090503035053/http://w2.eff.org/Privacy/Surveillance/CALEA/?f=archive.html). Electronic Frontier Foundation. Archived from the original (http://w2.eff.org/Privacy/Surveillance/CALEA/?f=archive.html) on 3 May 2009. Retrieved 14 March 2009.
119. "CALEA: The Perils of Wiretapping the Internet" (https://www.eff.org/issues/calea). Electronic Frontier Foundation. Retrieved 14 March 2009.
120. "FAQ on the CALEA Expansion by the FCC" (https://www.eff.org/pages/calea-faq). Electronic Frontier Foundation. 2007-09-20. Retrieved 14 March 2009.
121. Cauley, Leslie (11 May 2006). "NSA has massive database of Americans' phone calls" (https://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm). *USA Today*. Retrieved 12 May 2010.
122. Erin Mahoney and Joanne Helperin (3 July 2009). "Caught! Big Brother May Be Watching You With Traffic Cameras" (http://www.edmunds.com/ownership/driving/articles/42961/article.html). Edmunds. Retrieved 19 September 2013.
123. "Law Enforcement Operations" (http://www.persistentsurveillance.com/lawenforcement.html), Persistent Surveillance Systems. Retrieved 9 September 2013.
124. Savage, Charlie (12 August 2007). "US doles out millions for street cameras" (http://www.boston.com/news/nation/washington/articles/2007/08/12/us_doles_out_millions_for_street_cameras/?page=full). *The Boston Globe*. Retrieved 19 September 2013.
125. McFadden, Robert D. (7 August 2007). "City Is Rebuffed on the Release of '04 Records" (https://www.nytimes.com/2007/08/07/nyregion/07police.html?ref=nationalspecial3). *New York Times*. Retrieved 5 April 2010.
126. van der Vlist, Fernando N. 2017. Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden. Surveillance & Society 15(1): 137-157.
127. "Country Report: Socialist Republic of Vietnam" (http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line%20vFINAL.pdf), *Safety on the Line*, Cormac Callanan and Hein Dries-Ziekenheiner, Freedom House, July 2012. Retrieved 19 September 2013.
128. Arrington, Michael (15 May 2008). "He Said, She Said In Google v. Facebook" (https://techcrunch.com/2008/05/15/he-said-she-said-in-google-v-facebook/). TechCrunch. Retrieved 14 August 2009.
129. Papakipos, Matthew (28 May 2009). *"Google's HTML 5 Work: What's Next?" (62 minute video)* (https://www.youtube.com/watch?v=AusOPz8Ww80). *Google I/O 2009*. YouTube. Retrieved 19 September 2013.
130. "Google CEO bullish on mobile Web advertising" (https://www.reuters.com/article/idUSL2563364020080125). Reuters. 25 January 2008. Retrieved 28 February 2010.
131. Schmidt, Eric (16 February 2010). *Keynote speech (video)* (https://www.youtube.com/watch?v=YuqiE2lukDM). *2010 Mobile World Congress Barcelona*. YouTube. Retrieved 28 February 2010.

132. Schmidt, Eric (16 February 2010). *Keynote speech (video)* (https://www.youtube.com/watch?v=BuzSOo50XSg). *2010 Mobile World Congress Barcelona*. YouTube. Retrieved 28 February 2010.
133. "Content distribution regulation by viewing use" (http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220120278904%22.PGNR.&OS=DN/20120278904&RS=DN/20120278904), Microsoft Corporation, United States Patent Application 20120278904, 26 April 2011. Retrieved 19 September 2013.
134. Manuel Castells, (August 2009), *The Rise of the Network Society* (http://www.wiley.com/WileyCDA/WileyTitle/productCd-1405196866.html), 2nd edition, Wiley Blackwell, ISBN 978-1-4051-9686-4. Retrieved 23 September 2013.
135. "Smart cities? Tell it like it is, they're surveillance cities" (https://www.theregister.co.uk/2017/09/07/smart_cities_are_surveillance_cities/).
136. The first use of the term "electronic police state" was likely in a posting by Jim Davis "Police Checkpoints on the Information Highway" (http://cu-digest.org/CUDS6/cud6.72). *Computer Underground Digest*. **6** (72). 11 August 1994. ISSN 1066-632X (https://www.worldcat.org/issn/1066-632X). "The so-called 'electronic frontier' is quickly turning into an electronic police state."
137. The term "electronic police state" became more widely known with the publication of *The Electronic Police State: 2008 National Rankings* (https://secure.cryptohippie.com/pubs/EPS-2008.pdf), by Jonathan Logan, Cryptohippie USA.
138. Kingsley Ufuoma OMOYIBO, Ogaga Ayemo OBARO (2012), "Applications of Social Control Theory: Criminality and Governmentality" (http://www.pdoaj.com/pdf-files/ijass,%20pp.1026-1032.pdf), *International Journal of Asian Social Science*, Vol. 2, No. 7, pp.1026-1032.

External links

- "Mass surveillance" (http://www.iep.utm.edu/surv-eth/). *Internet Encyclopedia of Philosophy*.
- "The State and Surveillance: Fear and Control" (https://web.archive.org/web/20111108000538/http://cle.ens-lyon.fr/08111026/0/fiche___pagelibre/%26RH%3DCDL_ANG100100), Didier Bigo and Mireille Delmas-Marty, *La Clé des Langues*, 23 September 2011,ISSN 2107-7029 (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:2107-7029).
- "Against the collection of private data: The unknown risk factor" (http://www.hbarel.com/index.php/against-the-collection-of-private). *Hagai Bar-El on Security*. 8 March 2012.