# How is big brother watching us media essay

'Big Brother' is a fictional character in George Orwells dystopian novel 'Nineteen Eighty-Four', which tells the story of one man's attempt to rebel against the totalitarian state in which he lives. In the society that Orwell describes, everybody lives under complete twenty-four hour surveillance by the governing authorities. Since the publication of Nineteen Eighty-Four, the phrase 'Big Brother' has entered the English language, to describe any attempts by governments to use mass surveillance.[1]

The main surveillance tool described in Orwell's novel is the imaginary 'telescreen', a cross between a television and a security camera[2], and in the past decade growing comparisons have been drawn between the imaginary telescreen and the Internet-connected personal computer that is in many modern homes.

The purpose of this essay is to investigate the mass surveillance of Internet communications carried out by western governments today, and the technologies used to carry out that surveillance. The essay will first look at the current privacy landscape in the USA, the European Union, and the UK, in terms of policies and legislation. Then it will discuss some of the most interesting technical methods used to carry out mass Internet communications surveillance.

The terrorist attacks on New York's World Trade Centre, of September 11th 2001, heralded the dawn of a new global political era. Following those atrocities and subsequent attacks in Egypt, the United Kingdom, Spain, Bali, Russia, Morocco, and Saudi Arabia, governments around the world have responded by tightening existing legislation and creating new anti-terror

laws. Many of the countries that changed their laws to combat terrorist threats also increased the powers of their law enforcement and national security organisations to perform communications surveillance and carry out electronic data search and seizure.

The 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001', more commonly known as 'The Patriot Act', was signed into law less than seven weeks after the Twin Towers attacks. The Act is organised into ten 'titles', including 'Title II: Enhanced Surveillance Procedures', and 'Title IX: Improved intelligence'. The Patriot Act, which was America's legislative response to the September 11th attacks, hugely increased American law enforcement and national security services' authority both in the USA and abroad. The Patriot Act strengthened immigration, banking, and money laundering laws. The Patriot Act also amended the Foreign Intelligence Surveillance Act (FISA) of 1978, which includes subchapters covering electronic surveillance and 'trap and trace devices' (used to capture non-content information regarding electronic communication). FISA was also expanded by the 'Intelligence Reform and Terrorism Prevention Act of 2004'.[3]

In July of 2002 the European Union passed the 'Directive on Privacy and Electronic Communications'[4]. This directive was amended in 2005 by the 'Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes' directive.[5]These directives will lead to European telecom firms being required to store data regarding the time and duration of all fixed line, internet, and mobile telephone calls, the location of mobile telephone calls, and details of all internet connections and

e-mail messages (although e-mail content is not recorded). The UK government was the prime mover in lobbying for this directive, stating that data was 'the golden thread' in terrorist investigations.[6]

We have seen then that current privacy landscape has been heavily influenced by the changing global political situation with specific reference to global terrorism. We know that legislation exists that allows western governments to carry out mass surveillance, but what do they actually do and how do they do it? Mass surveillance can take many forms, including physical surveillance in the form of identity systems, audio, video, RFID and satellite surveillance. Data surveillance can also be used in the areas of electronic commerce and public records.[7]For the purpose of this essay we will look specifically at some of the most interesting technologies (allegedly) used by government organisations to carry out mass surveillance of Internet communications.

One of the most infamous alleged mass electronic communication surveillance technologies is ECHELON, a top-secret Anglo-American collaboration tasked with gathering signals intelligence around the world. Although its existence is still officially denied the European Parliament commissioned a report in 2001 entitled 'on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)'[8]. They were sufficiently convinced of ECHELON's capabilities to recommend that European citizens and businesses should routinely encrypt their communications in order to maintain privacy[9].

The idea of the ECHELON network was supposedly agreed between London and Washington as far back as 1948, although its existence was not brought to public attention until the publication of New Statesman article in 1988. ECHELON's capabilities are the subject of much debate; some estimates report that it can sift through 90% of Internet traffic, though the European Union found that " the technical capabilities of the system are probably not nearly as extensive". The hardware used to collect the information also remains something of a mystery, with some sources claiming that ECHELON controls over one hundred satellites and dozens of ground based listening stations. Others point out that very little (<5%) of all Internet traffic travels via satellite, and that ECHELON necessarily controls 'packet sniffing' systems and fibre-optic taps placed secretly at public communications switches. [10]111213

The alleged widespread use of packet sniffing systems first came to light during congressional testimony in April 2000, when the FBI was forced to admit the existence of it's 'Carnivore' system, so called for its ability 'to get to the meat' of intercepted emails[14]. Carnivore was later revealed to have grown from an earlier FBI project called Omnivore, reportedly began in February 1997 but Omnivore itself probably grew from an even earlier project that still remains secret. Carnivore could be used in conjunction with two other pieces of software, called 'Packeteer' and 'CoolMiner', the three together being known by the FBI as the 'DragonWare suite'[15]. Carnivore was reportedly used to sift through the data of ISP's following the 9/11 outrages, although by this time it had been renamed to DCS1000 following adverse publicity[16]. It is generally thought that, if Carnivore was used at

this time, it was coming to the end of it's useful life as the FBI moved onto commercially available software, probably the NarusInsight™ suite[17].

Narus is an American company that describes itself as a " leader in providing the real-time traffic insight essential to profitably manage, secure and deliver Services over IP." However, Narus gained notoriety after its 'STA 6400' system was named in the 'Room 641A' scandal[18]. In May 2006 Mark Klein, a former AT&T technician, released statements alleging that he had discovered an illegal intercept facility, operated by the NSA, in room 641A of the AT&T building at 611 Folsom Street, San Francisco[19]. Mr Klein alleged that in 2003 AT&T built secret rooms in its premises in various American cities to house computer systems capable of allowing the American government to tap into AT&T's WorldNet service and the entire Internet. Mr Klein stated in his testimony " It appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the Internet, whether that be people's e-mail, Web surfing or any other data." USA Today later claimed that after 9/11, the NSA asked the large American telecommunications companies for access to their call records, and that at least the three largest, AT&T, Verizon, and BellSouth, had agreed. Although not listening to, or recording, the content of the calls, the NSA was allegedly tracking call data in order to analyse patterns for suspicious activity. The story alleged that the NSA's goal was " to create a database of every call ever made" inside America[20].

Although the nature of the governmental mass communications surveillance means that many of the claims made are 'alleged' rather than fact, it is certain that mass Internet communications surveillance does take place.

However, anyone who is familiar with modern cryptography might ask 'What is the point?' After all, easily available software such as 'PGP' is described by security expert Bruce Schneier as " the closest you're likely to get to military-grade encryption"[21]. Wouldn't any intelligent lawbreaker, especially an international terrorist plotting some outrage, simply encrypt their communications using a good privacy tool, such as PGP, and a 128-bit key (the maximum size allowed by US Government export policy)? According to accepted mathematical theory the computing power required to try all possible 128-bit keys in a brute force attack on an asymmetric key encryption algorithms is not only impossible, but will remain so for the foreseeable future[22]. Of course, in fact on average only half of those keys would be tried before the correct one is found, but again any terrorist or criminal could use a key size of 256-bits or even larger.

Such arguments have led to much speculation, on the Internet especially, as to the NSA's ability to crack asymmetric keys. In particular, the hypothetical hardware devices 'TWINKLE' and 'TWIRL', proposed by Adi Shamir of the Weizmann Institute of Science, would enable the factorisation of 1024-bit numbers in one year, if they were built[23]24. Rumours of the existence of such machines are fanned by reports that the United States has broken modern ciphers used by, amongst others, the Iranian intelligence service[25]. Although the European parliament report on ECHELON recommended that organisations and individuals use encryption to guard their communications against electronic eavesdropping[26], the report also led to the establishment of SECOQC[27], an organisation working for the " Development of a Global Network for Secure Communication based on

Quantum Cryptography". This seems to suggest that the European Union does not see conventional cryptography as the answer to secure communication, at least in the future.

So, in conclusion, it seems that the answer to the question 'Is Big Brother Watching Us', is quite simply yes. More pressingly, should we be worried about this mass surveillance, or are our governments only interested in protecting us from attacks such as those that shocked the world on September 11th 2001? Few people can argue that much of the legislative changes mentioned in the first part of this essay will make it more difficult for large-scale terror organisations to function. However, many of those new policies and laws also affect privacy and civil liberties. In the United Kingdom, for example, the threat of terrorism has been used to justify the introduction of national identity cards[28], even though the home secretary at the time of the London bombings, which killed more than 50 people in July 2005, admitted that I. D. cards would not have prevented them.[29].

Opponents of such laws argue that reduced authorisation requirements often weaken due process. At the start of this year Britain's 'Internet Service Providers' Association' (Ispa) singled out the UK for its role in pushing for Europe-wide data retention laws.[30]On the 10th of January 2006, then Home Secretary Charles Clark stated " Agreement on retaining communications data places a vital tool against terrorism and serious crime in the hands of law enforcement agencies across Europe." However, the UK government had originally proposed this policy in 2000 (over a year before the twin towers attacks) and at the time had been accused of deceiving the public over their proposals and of " duplicity" for lobbying for the law change

in Europe, yet publicly denying that it was seeking such sweeping powers. [31]

The United Kingdom is widely regarded as the Western democracy that subjects its citizens to the most surveillance.[32]In a graphic published by the Daily Telegraph on November 2, 2006, showing Privacy International's rankings of privacy protection around the world, Britain is described as 'the worst-performing western democracy'. In fact we manage to achieve the worst ranking available, classing the UK as 'an endemic surveillance society'. We share this dubious honour with Russia, China, and Malaysia, and achieve a 'worst countries' ranking in no less than six out of thirteen invasive national practices.[33]

Recent history has shown us that can and do abuse human rights. Although there is a clear and present need to fight terrorism we must have balance and control at the same time to ensure that democratic and legal due process is not weakened.