Infopack

EDITORIAL

APRIL, 2014

Popular Information Centre

# Increasing State Surveillance vs. Citizens' Privacy

*- Piyush Pant*

The governments of developing countries are increasingly under pressure to adopt the US programme of surveillance. The programme, though started post 9/11 terrorist attack on US World Trade Centre to counter the terrorist attacks, had other hidden agenda as well. And this hidden agenda was two-pronged i.e. profiling the citizens for the data-base to be used by the corporate in identifying consumer targets for their products and second,to enable the State security agencies to selectively use the data for branding innocent citizens as suspects in its 'fight against terrorism'. In the name of "National Security", the US began research and development of vast data-base containing the personal information, of every citizen. Beginning as early as 2004, the Bush administration had been secretly monitoring the e-mails messages, the internet searches and phone conversations of millions of Americans without their knowledge, the approval of Congress, or a warrant issued by a judge.

In the post-9/11 world, surveillance has increased to unimaginable degrees. Studies have shown how within a few weeks of terrorist attacks, almost 17 bills were introduced in the US Congress, including measures to tighten immigration, visa, and naturalization procedures. What is significant is that these bills allow tax-benefits to companies that use biometrics, and check employee backgrounds. This is also important to note that biometrics was tied up with the issue of identity and identification.

The surveillance of its citizens by the American State is done through a surveillance programme called 'PRISM'. It is a clandestine mass electronic surveillance data mining programme launched in 2007 by the National Security Agency (NSA). PRISM is a government code name for a data-collection effort known officially by the SIGAD US-984XN. It is said that the PRISM programme collects stored Internet communications based on demands made to Internet companies such as Google Inc. under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms. The NSA can use these PRISM requests to target communications that were encrypted when they traveled across the Internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier.

PRISM started in 2007 in the wake of the passage of Protect America Act under the Bush Administration. The programme is operated under the supervision of the U.S Foreign Intelligence Surveillance Court (FISA Court, or FISC) pursuant to the Foreign Intelligence Surveillance Act (FISA).

India, too, is on the way for acquiring its own version of PRISM. Already two surveillance entities have been floated to monitor Indian citizens' communications. The first, namely the 'Central Monitoring System', has already been set up in 2011. This system is used by the tax authorities and the National Investigation Agency to track phone calls, texts and emails to fight terror related crimes. The second, the 'National Cyber Coordination Centre (NCCC)' has already got the approval of the cabinet and will soon become the reality. NCCC will be used by a host of intelligence agencies including the National Security Council Secretariat (NSCS), the Intelligence Bureau (IB), the Research and Analysis Wing (RAW), the Indian Computer Emergency Response Team (CERT-In), the National Technical Research Organisation (NTRO), the Defence Research and Development Organisation (DRDO), the Army, Navy and Air Force, and the Department of Telecommunications to monitor all online activities to fight cyber crimes. The NCCC is expected to create real-time working assessments on cyber security threats, which will be able to put into operational action within a short period of the threat assessment being released. Developed at a reported cost of over Rs 1,000 crore, the NCCC is expected to involve all the internet service providers. However, questions still remain, within the public sphere, on the use of such agencies and how the sanctity of private data of users will remain uncompromised. These concerns have been amplified since India failed to detect mass data phishing by the US. According to a report, more than 6 billion pieces of data from India may have been already compromised by US agencies. That's why debate is going on in India as to how, through mass surveillance of all communication channels, the security concerns are having a head on collision with the Right to Privacy of Indian citizens.

This issue of **INFOPACK** is focused on summarizing the inherent dangers of increasing State Surveillance globally.

**Mass Surveillance and State Control: The Total Information Awareness Project**

By:

Elliot D. Cohen

First Published by:

Palgrave MacMillan, USA
2010

## Bird's Eye View

In the Introduction, the writer says that in George Orwell's famous novel '1984', the Big Brother kept 24 hours surveillance on all citizens of Oceana via a "telescreen" installed in every home, while the Ministry of Truth streamed in news and entertainment it deemed suitable for popular consumption.

In the novel '1984', the tripartite slogan of "The Party" is, "WAR IS PEACE; FREEDOM IS SLAVERY; IGNORANCE IS STRENGTH." These three ideological perspectives characterized what in this book is called a Culture of Control. Such cultures are characterized by an unequal power structure where one individual or group dominates another; hence, power flows in only one direction. In the political sphere, despotic, fascist states exemplify the idea of a culture of control. In contrast to a culture of control is a 'Culture of Autonomy'. Such a culture permits power to flow bilaterally.

While talking about **America as a Culture of Control**, the writer says that in the past decade, since the 9/11 attacks, America has largely moved in the direction of a culture of control. The tripartite characteristics of such a culture are reflected in the conventional wisdom that "winning the war on terrorism" is the route to peace; "freedom is not free" and, therefore, requires sacrifice, such as giving up civil liberties for the sake of safety (including relinquishing our right to privacy); and questioning authority, especially when it comes to national security, is unpatriotic and even treasonous.

Since the inception of the Bush administration in 2000, the rule of law has been severely compromised by the passage of "laws" enacted in the interest of "national security", that contravene the bill of Rights of the United States Constitution. This legislation includes laws that permit mass warrantless spying on Americans' electronic communications without adequate judicial oversight.

In the aftermath of the September 11, 2001 attacks on the World Trade Center and the Pentagon, in the name of "national security," it began research and development of a vast database containing the personal information of every citizen. Deploying this technology, beginning as early as 2004, the Bush administration had been secretly monitoring the e-mails messages, Internet searches, and phone conversations of millions of Americans without their knowledge, the approval of Congress, or a warrant issued by a judge.

The writer further points out that in 2008, Congress passed the Foreign Intelligence Surveillance Amendments Act to amend the 1978 FISA (Foreign Intelligence Surveillance Act), which had required a search warrant for any electronic communication passing through a US switch. Effectively, this new legislation gutted the 1978 Act and gave the green light to continue warrantless surveillance of millions of Americans. And soon-to-be President Barack Obama voted for it.

### A Plea for Constructive Change

The writer says that this book carefully examines the dangerous currents toward a controlled Orwellian culture now in the air. The TIA (Telecommunications Industry Association) Project cannot be servered from the political, legal, social, economic, technological, and ideological climate that now supports it. These factors include:

- The passage of laws permitting egregious violations of human rights;
- Federal courts - from FISA to the Supreme Court - falling asleep at the wheel;
- A "war on terror" used to promote the politics of fear and to justify increasingly greater abridgments of privacy;
- psychological manipulation aiming at mass, blind conformity, lock-step politics, and jingoism;
- corporate media consolidation, telecom mergers, and media-government quid pro quo;
- the consequent clogging and censoring of the arteries of mass communication;
- widespread and systematic injection of government propaganda into the mainstream media news hole;
- private data warehousing and mining companies working cooperatively with the US department of Defence to amass personal data on all of us;
- the military-industrial revolving door incestuously sustaining TIA technological development;
- corporate lobbies in Congress and the Federal Communications Commission seeking to undermine net neutrality;
- government monitoring of the internet;
- research and development of chilling late generation, privacy-eviscerating surveillance technologies;
- deployment of real time surveillance subsystems including video surveillance cameras in private zones;
- Secret Services death squads operating underneath the radar of Congress;
- A nationalistic, neoconservative ideology hell-bent on establishing and maintaining US geopolitical supremacy;
- Corporate globalization, breakdown of trade barriers, and the blurring of lines between political and corporate power, leaving a trail of exploitation of the world's labour force, destruction of the environment, and centralized means of world power and control in the hand of super-rich.

These are some of the factors that are indissolubly fused to the steady creep of a culture of control at the center of which is the TIA project.

In Chapter I, under the title **Post - 9/11 America's Culture of Control**, The writer says that the September 11, 2001, attacks on American soil were a decisive marker in the shift toward a culture of control.

**Restriction of Civil Liberties: The PATRIOT Act**, The writer says that the 9/11 attacks provided a pretext for restricting civil rights, especially privacy and the right to be kept informed. In particular, the US PATRIOT Act was approved by Congress without careful examination or discussion and was signed into law by George Bush on October 26, 2001.

Section 213 of the PATRIOT Act, the so-called "sneak and peek" provision, allowed law enforcement officers to search the homes or businesses of private citizens without their knowledge or permission.

Section 218 of the Act eliminated an important protection established in 1978 under the Foreign Surveillance Act (FISA) against warrantless surveillance of American citizens and violation of their Fourth Amendment rights. In particular, Provision 104(7) (B) of 1978's FISA required that the purpose of conducting a warrantless electronic surveillance was to obtain foreign intelligence information.

Section 215 of the PATRIOT Act gave the Federal Bureau of Investigation (FBI) the power to access the "tangible things" of private citizens including their "books, records, papers, documents and other items" through the issuance of National Security Letters (NSL). These letters did not require a court order. All the FBI had to claim was the surveillance was being conducted "to protect against international terrorism or clandestine intelligent activities."

Under the title of **Fear and Hate Mongering**, the writer says that the rallying cry of the Bush administration was that of giving up civil liberties for the sake of peace and security. American support for the war in Iraq was largely a product of such fear-mongering rather than the higher reflective powers of a democratic nation. Thus Saddam Hussein was a pretext used by the Bush administration to stir up support among Americans for the invasion of Iraq. And when the Bush administration fabricated a link between Hussein and the 9/11 attacks, most Americans came on board; and most were also willing to consent to having their electronic communications warrantlessly wiretapped for the sake of averting the next terrorist attack.

While talking about **Manipulation of Mainstream Media and Telecoms**, the writer says that it is not just

the average American who is subjected to being manipulated; the mainstream media is, and has also been so subject. Giant media corporations have come under government influence or control. A relatively few number of companies now control all of cable and network (New Corp, General Electric, Viacom, Disney, and Time Warner being the prominent conglomerates). All these companies are beholden to the government for media ownership caps, mergers, tax breaks, military contracts, and other means of expanding their bottom lines. They also have lobbies in Congress and the Federal Communications Commission (FCC) and are, therefore, disinclined to report news that strain their relationship with the government.

The writer further says that an instructive example of what can happen to a company that refuses to cooperate with government is that of Qwest Communications, which refused to assist the Bush administration in its warrantless surveillance programme. According to the former CEO of Qwest, Joseph P. Nacchio, the Bush administration had withdrawn lucrative government contracts due to Qwest refusal to comply with the directive to cooperate in its programme.

In the context of The **Net Neutrality Crisis**, the writer says that the Internet is also in clear danger of becoming another branch of the corporate, mainstream media. Currently, there are powerful telecommunication companies such as Comcast seeking to turn the free and open architecture of the net into a "pay and play" system according to which only companies that have deep pockets would be able to afford an Internet presence. Consequently, these companies, which include the major cable and broadcast media corporations, would have the ability to control, censor, and otherwise manipulate the flow of information through the Internet pipes. This would mean the end of net neutrality and a brave new world of Internet control.

At the center of America's trend toward a controlled society is a project began in the early years of Bush administration originally called, "Total Information Awareness" (TIA). The TIA project represents another formidable move by the Defence Advanced Research Projects Agency (DARPA) toward a culture of control. This project involves construction of a vast database of personal information (from movie rentals and credit card purchases to phone and e-mail conversations) and a network of integrated technologies for trolling through it.

Chapter II refers to **The Total Information Awareness Project**. Under this title, the writer says that the control of information is the cornerstone of a controlled society. For any government bent on controlling its subjects, this control is double edged. First, the government must know everything it can possibly know. Second, everyone other than the government must not know what the government knows. This was exactly the approach taken by the Bush administration in the aftermath of the 9/11 attacks, and the double-edged edifice of control it established is still alive and flourishing.

After the 9/11 attacks, on October 30, 2001, the DARPA, a branch of the Department of Defence, established the "Office of Strategic Influence" (OSI) (otherwise known as the "Office of Disinformation") for similar purposes. The official purpose of OSI was to disseminate false information to America's foreign "enemies", especially Islamic nations, by spreading disinformation through their media networks, the Internet, and covert operations.

However, these surreptitious attempts to control information did not stop at infiltrating foreign media. At this time the Bush administration was also aggressively disseminating pro-war and pro-Bush propaganda into the American mainstream media. In fact, the Bush- administration paid millions of tax-payers' dollars to produce and disseminate phony news favourable to its policies and image.

The writer further points out that the TIA technologies consisted of an integrated system of technologies including the following:

*Genesis:* technology that permits the storing and organizing vast amount of data;

*Evidence Extraction and Link Discovery:* these technologies extract data from multiple sources (such as text messages and Web pages);

*Scalable Social Network Analysis:* technologies that distinguish possible terrorists from innocent civilians. This means that the latter group must be placed under surveillance and subjected to analysis along with the former group.

*Human ID at a distance:* automated biometric identification technologies to detect, recognize, and identify humans at great distances. In fact, in February 2008, at a cost of one billion dollars per year, the FBI awarded

a ten year contract to Lockheed Martin to develop a giant database of biometric data including fingerprints, iris scans, and DNA. The goal is to have such personal data from every human being on file.

*Effective Affordable Reusable Speech-To-Text:* Such technology is necessary to construct a massive dragnet surveillance of telephone and Voice/IP communications;

Translingual Information Detection, Extraction, and Summarization: this technology enables English speakers to find and interpret critical information in multiple languages;

*Communicator:* technology that enables warfighters to talk with computers, such that information will be accessible on the battle field or in command centers;

*Wargaming the Asymmetric Environment:* this is to better anticipate and act against terrorists by identifying predictive indicators of attack;

*Future markets applied to prediction:* technology to help predict political instability, threats to national security, and other major events in the near future.

The writer says that, in fact, such a functionally integrated TIA system was deployed by the NSA to spy on the telephone and e-mail conversations and Internet activities of millions of Americans.

**The National Security Agency's Deployment of the TIA System**

Russell Tice, who was an NSA intelligence officer until 2005, alleged that the NSA surveillance programme had routinely parsed through all faxes, phone calls, e-mail exchanges, and Internet searches of every American. According to Tice, the NSA had kept a file on every American citizen, and each file contained not only communications data but also credit card information and other financial data. He further said that the NSA had expressly targeted US journalists for purposes of collecting their data.

In 2006, a former AT&T technician, Mark Klein, alleged that the NSA was conducting a massive dragnet of all electronic communications of American citizens starting in 2003. Klein maintained that the NSA had built a secret room and housed computer equipment in it. This computer equipment was connected by fiber optic splitters that tapped into the circuits through which messages throughout the nation and the rest of the world flowed. This meant that all messages, both domestic as well as international, were being copied and parsed by the NSA according to predefined, secret definitions.

The writer further says that there is no technological means of eliminating the possibility of terrorist attack. A more sober question is whether the degree of protection that might possibly be gained through the use of TIA technologies is worth the abridgement of civil liberties arising out of such use.

Technological problems aside, warrantless, wholesale spying operations were never legal. Nor should they have been, because they are inconsistent with the Fourth Amendment, which forbids unreasonable searches and seizers without warrant or probable cause.

Bush's warrantless surveillance programme was in clear violation of the 1978 FISA. This is because, pursuant to this law, messages passing through US switches could not be tapped without a court warrant. Unfortunately, this inherently unconstitutional programme was subsequently turned into law, at first in the form of the 2007 Protect America Act, and later in the form of the 2008 FISA Amendments Act. These laws have given an air of legitimacy to what should never have been legal in the first place.

In Chapter III, the writer talks about **Legal Pretexts for Continuing the TIA Project**. He says that the Bush administration made changes to spy laws that have given a veneer of legality to the TIA Project and helped ensure its survival into subsequent government administrations. There were at least three major legal reforms by the Bush administration between the months of July and October 2008 that were largely responsible for these constitutional abridgements. These are:

1. On July 10, 2008, with the approval of Congress (including that of soon-to-be President Obama), President Bush signed into law the FISA Amendments Act of 2008 (H. R. 6304), which downgraded the role of the FIS Courts and gave giant telecom corporations both retroactive and retrospective legal immunity, thereby building a legal shield around Bush's unlawful past programme of warrantless, mass surveillance; and, effectively, permitting it to operate, in the future, outside the radar of the judiciary.
2. On July 31, 2008, President Bush placed on the White House Web site an amended version of Executive Order 12333, a directive that was first issued in 1981 by the Reagan administration. The newly amended

version established the Director of National Intelligence (DNI) as the "head of the intelligence community." The Order also gave the Attorney General (AG) the power to spy on persons inside the United States as well as US citizens abroad without a warrant.

3. On October 1, 2008, the latest assault on privacy and the rule of law came in the form of revised FBI rules that permit racial profiling as a basis for spying on America.

The writer further says that these laws have set the stage for continuing the TIA project began during the Bush administration and for moving America further down the road of a culture of control.

Unfortunately, not only does this Act (H.R. 6304) grant immunity from civil action to all telecommunication companies that participated in the President's warrantless surveillance programme during the period beginning of September 11, 2001, and ending on January 17, 2007, it also unconditionally releases these companies from any future liabilities (presumably both civil and criminal). For it unqualifiedly states "No cause of action lie in any court against any electronic communication service provider for providing any information, facilities, or assistance.

The Act also pre-empts state investigations into the allegedly illegal activities of these companies in assisting the intelligence community, and from requiring through regulations or other means disclosure of information about such assistance. The courts as well as the states are, therefore, barred from fulfilling their respective roles in protecting the public from encroachment of civil liberties by federal agencies, and by the telecommunication companies working in concert with these agencies.

Pursuant to H.R. 6304, in as much as American citizen can no longer file suit against the telecom companies for past and future violations of their Fourth Amendment right to privacy.

However, today much of the world's electronic communications pass through fiber-optic networks located in the United States, even in cases where both parties to the communication are located outside the country. Because the 1978 FISA was understood to require the government to obtain a court warrant whenever the communication was routed through the United States, this means that such foreign communication also required a warrant. So, proponents of FISA reform argued that exiting law needed to be changed in order to permit warrantless surveillance of foreign communications routed through the United States.

**The New FBI Rules**

The writer says that coming on the heels of the FISA Amendments Act and Executive Order 12333 are the revised FBI guidelines signed into law on October 1, 2008, by Attorney General Mukasey. These rules purportedly allow the FBI to use racial criteria in conducting its terrorism investigations. With this new law in place, not only is such digitized racial profiling not subject to direct FIS Court inspection pursuant to H.R. 6304, it is also legal.

In addition to permitting racial profiling, these new guidelines allegedly permit the FBI to undertake surveillance without probable cause, based on the vague grounds of a perceived "threat". They also allegedly permit the use of intrusive investigative techniques such as undercover interviews, the use of informants, and physical surveillance to investigate individuals planning a public demonstration, an activity that is supposed to be protected by the First Amendment.

Chapter IV is titled - **The Foreign Intelligence Surveillance Court Review: Purveyor of "Double Think"**. In this chapter, the writer says that The Foreign Intelligence Surveillance Court of Review (FIS court), which has the power to review petitions made by telecommunications companies, now seems to have become afflicted with "double think." Because the court has recently set the dangerous precedent of taking the word of government officials, indeed taking it on "faith", that they would not infringe the constitutional right to privacy of millions of Americans, although there is a body of contradicting evidence. Instead of considering this evidence, the Court cleansed away the contradiction simply by ignoring it. The legislative branch of government has not, to date, considered the dangerous dynamic of having approved legislation that exempts telecommunications companies from the usual criminal and civil liability in order to make them accomplices to mass, warrantless spying on millions of Americans.

The telecom companies' participation in such a programme is now "legally" coerced. According to the FISA Amendment Act of 2008, the Attorney General (AG) and Director of National Intelligence (DNI) may direct a telecom company to "immediately provide the Government with all information, facilities, or assistance

necessary to accomplish the acquisition (of foreign intelligence).

**Compelled to Spy: The Case of Quest Communication**

The writer says that on August 22, 2008, the three-member FIS Court of Review granted a motion by the Bush administration compelling a telecommunications company to participate in the National Security Agency (NSA) warrantless surveillance programme.

The company in question, Qwest Communications, had refused to comply with the Bush administration's directive on the grounds that the programme would have been in violation of Fourth Amendment rights of its customers. The directive was issued pursuant to an amendment to the 1978 FISA called the Protect America Act (PAA), which became law on August 5, 2007. The court concluded that the directive, which was issued at the time the PAA was in force, was lawful.

Ironically, just six days after the Court publicized its decision, and one day after Bush left office, former NSA officer Russel Tice claimed that the surveillance programme had routinely parsed through all faxes, phone calls, e-mails exchanges, and Internet searches of every American.

But even before Tice came forward, as early as November 2007, a former AT&T technician, Mark Klein, claimed that the NSA was conducting a massive dragnet of all electronic communications of American citizens. Klein had carefully documented his claims. This documentation included photographs and diagrams describing the surveillance equipment installed at the San Francisco AT&T hub where Klein had worked.

Nevertheless, the FIS Court of Review did not address the constitutional challenge raised by the possibility of such spying on Americans. On August 22, 2008, "the risks of error and abuse are within acceptable limits. Yet, given the massive dragnet described by Klein, it was unclear how it could have been so unequivocally concluded that the risks of error and abuse were within acceptable limits.

The writer further says that according to the former CEO of Qwest, Joseph P. Nacchio, the Bush administration had withdrawn lucrative government contracts due to Qwest's refusal to comply with the directive to cooperate in its warrantless surveillance programme.

In any event, because the prosperity and even survival of giant telecom companies depends upon government, these companies are currently in both a legal and financial stranglehold by the federal government. It is, therefore, predictable that these companies, acting to expand or protect their bottom lines, will, in the future, assist the government in regularly conducting mass spying operations on millions of Americans. Moreover, since controversial provisions have been included in the 2008 FISA Amendments Act, which grant retroactive and future legal immunity to telecoms, American citizens are now barred from filing suits against these companies for assisting the government in spying on them.

In addition, in April 2009, the Obama Justice Department has gone even further than the Bush administration in closing off avenues for citizens to seek redress for violation of their Fourth Amendment rights.

In Chapter V under the title-**The Military-Industrial Information Network**, the writer says that much of the personal data collection that feeds the government's Total Information Awareness (TIA) project is not directly obtained by government. Instead, data such as credit card purchase histories, medical records, bank records, airline ticket information, car rentals, and utility bills (among other digitized information) is collected by companies who are not subject to the same legal constraints as the federal government. The government then, in turn, contracts with these companies to tap into their massive databases. In this way, government is able to circumvent privacy such as court warrants.

The private sector is therefore helping the federal government to actualize two essential, integrated functions of the TAI system: data warehousing and data mining.

The writer further says that the process of data warehousing and data mining have become lucrative businesses for private military contractors. One data warehousing company that played a major role during the Bush administration in aiding implementation of the TAI project was ChoicePoint, Inc. After the September 2001 attack, it shifted its focus from commercially available products to homeland defence. This company also maintained a strategic alliance with Department of Defence contractor, Science Applications International Corporation (SAIC). SAIC was the architect of the main brain of TAI.

According to the National Journal, the ChoicePoint for access to its vast databases, which contained "billions of personal records about nearly every person-citizens and non-citizens alike-in the United States." Moreover,

according to this report, federal documents obtained by the National Journal and Government Executive, ChoicePoint provided the FBI and Department of Defence access to a "previously undisclosed, and vaguely described 'exclusive' data-searching system". According to said documents, in early 2003, the agencies also ordered Internet-based services from ChoicePoint, "effectively put the power of the company's databases at government agents' fingertips on their desktop computers." The government also purchased access services from ChoicePoint such as AutoTrackXP, which can "provide Internet access to more than 17 billion current and historical records on individuals and businesses, and allow users to browse through those records instantly" and with a little information as a name or Social Security number to cross-reference public and proprietary records. ChoicePoint also developed Consolidated Lead Evaluation and Reporting (CLEAR), a second generation AutoTrackXP product especially for the use by government and law enforcement.

It is worth emphasizing, however, that ChoicePoint warhouses are only one component of a massive, integrated TIA data reservoir, which also includes: all of the electronic messages and internet searches collected by the NSA with the help of the telecom companies; the biometric data contained in the FBI's biometric database; and video data obtained from surveillance cameras situated in major cities.

In this context, the writer also mentions the name of Thomson Reuters, another giant information company, one of the world's largest news services providing worldwide news to newspapers and mainstream media organizations. Having been known for its objectivity, unbiased reporting, and strict code of ethics, Reuters is now part of conglomerate that sell databases containing the personal information of American citizens to the federal government.

However, companies such as ChoicePoint and Thomson Reuters are less formidable violators of privacy than companies such as Google. This is because the former companies are quite candid about the fact that their primary business is to amass personal information. Not so with companies like Google.

For millions of Internet users, entering search terms into Google's search engine is seen as a way of acquiring information. In fact, from the perspective of Google, Internet users are not primarily consumers of information. They are themselves sources of incredibly personal information.

The writer further says that Google's main reason for "tracking user trends" is to amass behavioral information for purposes of targeted online advertising, its main source of revenue. In 2007, for this purpose, Google merged with DoubleClick, a major provider of digital marketing technologies and services.

Hence, merger between Google and DoubleClick has enabled the team to combine user information collected by DoubleClick technologies with search histories gathered by Google to create a massive database of consumer information. This in turn leaves Internet users vulnerable to having their *Internet identities or profiles* accessed by the federal government and linked to the other personal data it has amassed.

However, the increasingly close business ties that Google now enjoys with federal agencies makes it likely that the information giant will cooperate with government demands for information in the future. For example, more recently, Google has partnered with NSA, CIA, and FBI to create an intelligence database that lets these agencies share information with each other. Such close-knit relationship with these federal agencies along with the lucrative defence contracts it stands to gain (or lose) makes cooperation a probable option for a giant corporation like Google with an immense appetite for profit.

The writer also points out that the rise of social media such as Twitter and facebook marks a trend toward a culture of autonomy and away from a culture of control. Unfortunately, there are reasons to think that at least some social media have in fact been created for the opposite purpose; that is, to leverage state control over inter-personal communication. At least, so it seems in the case of Facebook. Facebook is presently the world's largest social media network with over 350 million users. Its fast-growing popularity among college students attracted the attention of entrepreneurs with high-level connections in the federal government. It received its first financial backing in the form of an US$500,000 in late 2004 by Peter Thiel.

Then 350 million users of Facebook are being used as experimental subjects by the government without their informed consent. There are technologies that place innocent masses under surveillance in order to acquire information about their behavioral patterns. Facebook is DARPA's tool for collecting data on the masses in order to construct algorithms to distinguish anomalous, terrorist cases from usual ones. Such mass spying contravene respect for privacy.

Under the topic titled-**Web of Deceit: The Tenuous Future of Net Neutrality**, the writer says that

according to a December 2008 Pew Research Survey, the Internet has surpassed all other media except television as an outlet via which people receive national and international news. There is also an expanding presence of major media corporation on the Internet. Most people get their Internet news from a mainstream corporate media Web site like Fox.com or MSNBC.com. What this suggests is that the absorption of TV into an expanding cyberspace may also mean greater and greater corporate control over of the Internet, and less and less Internet freedom and democracy.

Now unfolding is a legal-political-corporate current moving closer to turning a vibrant, democratic Internet into a global extension of the corporate mainstream media, which would portend a web of manipulation, censorship, and control over information. The signs exist, but the stakeholders (the federal government and a small group of interconnected, powerful telecom and mainstream media monopolies) have kept them from public awareness. Indoctrinated and sealed off from the outer world, you will inhabit a matrix where every ounce of creative, independent thinking that challenges government policies and values will be quietly squelched. The corporate mainstream media have been quiet about the telecom lobbies in Washington, and the filing of suits in state and federal courts to halt production of community Internet, all aimed at monopolizing and controlling the net. So-called "net neutrality" is being challenged by the giant telecoms like Fox News and CNN.

**The Global Firewall: Internet as a Military Weapon of Mass Deception and World Domination**

In this context, the writer says that in 1997, a neo-conservative think tank emerged called The Project for the New American Century (PNAC). Its main mission was to promote corporate globalization and the increase in US military dominance throughout the world. This included defeating all regimes opposed to US corporate interests. In its blueprint of what would be required for the transition, it stressed the necessity of government control of the Internet.

The writer further says that we have witnessed the erosion of privacy through the passage of Total Information Awareness (TIA) programme. Technologies are already being harnessed to police the Internet and e-mail activities of American citizens. It is not much of a stretch from here to suppose that government is (or soon will be) blocking and constraining content it deems an affront to "national security". At the present juncture, in light of the aforementioned legal, political, and corporate realities, it is also not difficult to envision the progressive stages the net might undergo in being transformed into a vehicle of world domination:

**Stage 1: Corporatizing the Net**

The Brand X Supreme Court decision has already "corporatized" the Internet by giving telecom and phone companies like Comcast and AT&T the authority to control the Internet pipes;

**Stage 2: Sanitizing/Propagandizing the Net**

The conventional mainstream news venues (broadcast television, cable, radio, newspapers) are engaged in "information warfare" and "perception management". Such firms have screened embedded journalists on the basis of how supportive they have been of government war policy; injected government propaganda into foreign press; placed phony news into local network affiliate coverage; recruited "military analysts" to use as "Trojan Horses" for injecting government propaganda into network and cable television news programming; used top secret National Security Agency (NSA) clearance to spy on journalists using powerful TIA surveillance equipment;

**Stage 3: Militarizing the Net**

Stage 3 is the transformative level envisioned by the PNAC. It would involve harnessing e-mail and web-filtering technologies not merely to intercept and disable service attacks, viruses, and other attempts to shut down the Internet. It would also involve deployment of content-filtering technologies using sophisticated algorithms to block e-mail and web transmissions of whatever is deemed to "national security".

By the mid 1990's, content-filtering technologies had in fact become a major interest of the Department of Defence (DOD). If used by the DOD to enforce government policies and protect "national security", such "news filtering" technologies could render the First Amendment right to freedom of the press null and void.

**Stage 4: Globalizing the Net**

The writer says that this last stage in the progression toward state control of the Net involves encapsulating

the world, or as much of it as possible, behind a "Global Firewall" managed by government with the cooperation of the telecommunication giants. As conceived by PNAC, this stage would use corporate globalization as a mechanism to attain US military dominance throughout the world. According to this vision, the Internet would figure as a key element "in global commerce, politics and power"; for whoever controls the Internet (and Cyberspace) has a decisive advantage in attaining global control.

It is clear that the giant telecom and phone companies, such as Comcast and AT&T are poised to play decisive role in helping the United States or some other politico-corporate world organization attain global, cyber-dominance. These companies already assist in monitoring all electronic communications that pass through American switches. They are also prepared to control the content of the Internet through a system likely to be dominated by mainstream corporate media Fox, NBC, CBS, ABC, and CNN.

Under the topic titled-**Echelon: The Global Total Information Awareness Network**, the writer says that progress has been made to encapsulate the world inside a global, transnational TIA network. Since the 1970s, during the cold war with the Soviet Union, the US government has spearheaded a partnership with the United Kingdom, Canada, Australia, and New Zealand to expand its surveillance capabilities globally. This involved deployment of "Echelon", the code name for a massive global surveillance network for data capture, exchange, and analysis. A 2001 European Parliamentary investigative report described the system as follows:

"Within Europe, all e-mails, fax, telephone communications are routinely intercepted by United States National Security Agency, transferring all target information from the European mainland to The Headquarter of NSA….a global surveillance system that stretches around the world to form a targeting system on all of the key Intelsat satellites used to convey most of the world's satellite phone calls, internet, emails, faxes, telexes. Unlike many of the electronic spy systems developed during the cold war, ECHELON is designed for primarily non-military targets: governments, organizations and businesses in virtually every country. The above-mentioned five nations share the results with the US as the senior partner."

So the destruction of net neutrality and, ultimately, the commandeering (and hijacking) of the Net by the State is an even more serious and devastating assault on democracy than that which has taken place elsewhere in the mass media.

Chapter IX refers to the topic titled-**War is Peace: The War on Terror**. In this context, the writer says that the key idea is that, by embroiling a nation in perpetual war, the ruling party is able to keep the masses ignorant, poor, and dependent on government. This is because war economies direct production to military arsenals instead of education, health services, and other services, and other social goods that could otherwise have improved the lives of the masses.

The writer also says that war is not fought to be won. In the case of Oceana, war was unwinnable because there were two other superpowers that were equally matched to itself in power.

Ironically, depicted in this fictional account of war are some salient features of waging a "war on terror" in twenty-first-century America. The features are:

1. Like Oceana's war, such a "war" is, in principle, incapable of ever being won, because it is impossible to ever completely eradicate terrorism. A war on terror is therefore, in principle, endless.
2. Like the enemy in Oceana, the enemy in war on terror is obscure and subject to change. In a global war on terror, virtually anyone and everyone can be branded a "terrorist" or "unlawful enemy combatant", including, for example, an antiwar protester. Accordingly, Saddam Hussein provided such an excuse for the Bush administration to invade Iraq.
3. In twenty-first-century America, the idea of war that cannot be won finds its protractors in those who wield money and power. Thus, for the corporate CEO, the gains of war are largely aimed at feeding the corporate appetite for profit. Therefore, the longer the war lasts, the more profitable it becomes. In this manner, a war on terror, which is perpetual war, is a corporate bonanza.
4. However, the present war on terror has helped the corporate sector to expand its bottom line at the expense of the masses. On October 2009, President Obama signed the largest military budget in world history, US$680 billion for the Pentagon.

   On the other hand, such enormous military budgets portend reduction in funding for social services, education, and other non-military employment opportunities. The tendency of a war economy aimed at fighting a

perennial war on terror is to support big business, especially military contractors.

5. In this climate of perpetual war on terror, war ceases to exist and becomes a state of peace wherein we, as Americans live in a self-contained universe, "freed from the sobering influence of external danger." However, this "freedom" must be purchased at the cost of relinquishing our civil liberties, especially privacy.
6. Mass, warrantless surveillance is, therefore, a necessary corollary of war and terror. In order to hunt down and capture terrorists, it is necessary that government have the technological means of mass search and seizure. It is in this manner that the current war on terror has provided the pretext for the systematic invasion of privacy of millions of Americans (indeed billions of human beings throughout the world) through mass, warrantless surveillance.
7. The current war on terror is based on mass manipulation and deception. It has been sold to the American public on the basis of wholesale fabrication of the rationale for going to war in the first place. The true basis for this pretext has not been to protect the borders of America against future terrorist attacks. The primary reason has instead always been the amassing of geopolitical power and world dominance.

In Chapter X, under the topic titled-**Obama's War on Terror: Not Change We Can Believe In**, the writer points out that on January 22, 2009, speaking at the State Department, Obama stated, "We are confronted by extraordinary, complex and interconnected global challenges: war on terror, sectarian division and the spread of deadly technology. We must bear it." Obama made clear that he expected all Americans to accept the "global" challenge of a "war on terror".

The write further says that in fact, the war on terror is a product of fabrication of an aggressive media blitz and public relation initiative launched by the Bush administration in the aftermath of the 9/11 attacks, which exploited these attacks for purposes of frightening, intimidating, and indoctrinating Americans into surrendering their civil liberties and rallying around the flag.

Nevertheless, Americans have been successfully indoctrinated to believe that they are immersed in the fighting of a legitimate, real war, and that, as President Obama admonished, "we must bear it." Thus, in a May 2006 Washington Post poll, when asked if, for purposes of detecting terrorist activities, they would allow the NSA to keep track of every phone call (both domestic and foreign) they made and received, about two-third of Americans polled said it would be all right. They were willing to accept such an invasion of privacy, notwithstanding that it was illegal, for the sake of preventing another terrorist attack.

While talking about **Unmasking the War on Terror**, the writer says that a key mechanism of this global initiative is the doctrine of preemptive war. "Preemptive" here is largely euphemistic for wars fought to advance the economic and political interests of America in the maintenance of its preeminence as the world's sole superpower.

In its report on Rebuilding America's Defences (RAD), The Project for the New American Century (PNAC) clearly laid out some of the main objectives under girding the preemptive war strategy. Unfortunately, these objectives, which were initiated during the Bush administration, have to a significant extent been embraced by the Obama administration.

RAD also emphasized the need to "transform US forces to exploit the revolution in military affairs." This included the design and deployment of a global ballistic missile defence system consisting of land-, sea-, air- and space-based components said to be shielding the US and its allies from "limited strike" in the future by "rogue" nations, such as Iraq, North Korea, and Iran.

Here, the interest in such missile defences was not that of shielding the homeland from an unprovoked missile but rather the interest in such defences was to allow the United States to carry out "preemptive" wars and other aggressive military and political actions aimed at world domination.

In this context, the writer also talks about **Control of Space and Cyberspace**. He says that PNAC's quest for world domination transcends any literal meaning of the geopolitical, and extends also to the control, rather than the sharing of outer space. Moreover, it also has serious implications for cyber freedom. Thus, RAD also states , "Much as control of the high sea - and the protection of international commerce-defined global power in the past, so will control of the new "international commons' be a key to world power in the future."

However, there is a difference between protecting the Internet from a cyber attack and controlling it for purposes of amassing "world power." The former is defensive and the later is offensive. Obama administration

established the National Cybersecurity Communications Center (NCCIC), which has been described as "a 24-hour, DHS-led coordinated watch and warning center that will improve national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure.

In fact, the NSA will be involved in operation of the NCCIC, whose principle role will be "to monitor and assure the security and safety of civilian-government computer networks and to provide early warning to private businesses about cyber-attack threats." Clearly, the NSA's role in monitoring private civilian computer networks as well as military ones represents a dangerous concession to state control of cyberspace.

The writer further says that without the camouflage of fighting a war on terror, the TIA project will be defused; for the official reason for conducting a warrantless, dragnet of everybody's personal electronic communications is the hunt everywhere and anywhere for terrorists. Without a "war on terror", convert operations to locate international criminals can be conducted as it had been pursuant to the 1978 Foreign Intelligence Surveillance Act, namely by search warrants approved by a FIS Court. Thus, the claimed need for FISA reform in the first place has been largely misrepresented.

Unfortunately, the Obama administration has not surrendered the idea of fighting a war on terror, and it has shown no signs of dismantling the TIA system or of taking a lead in reforming the current FISA laws.

Chapter XIII refers to topic titled-**Big Brother is (literally) Watching You: The Manhattan Security Initiative**.The writer says that America has become a culture fixated on fighting a bogus "war on terror". National fear and apprehension about the possibility of the next terrorist attack have made average Americans receptive to increasing levels of government interference with their civil liberties. Americans have now become desensitized to having their personal e-mail and phone messages searched by the National Security Agency (NSA). They have accepted the fact that any books that they purchase on a credit card or check out from the library will be added to an NSA database along with credit card, healthcare, and financial information.

In 2007, New York City began its "Lower Manhattan Security Initiative", which, when completed, will a network of some 3000 television cameras "designed to help ensure public safety and security, and to detect, deter, and prevent potential terrorist attack." The system also includes chemical radiological sensors intended to detect potential terrorist threats; and it includes license plate readers, which can zoom in on license plates of suspects.

The writer further says that while video cameras have previously been used in public and private areas for crime prevention and monitoring, the new technology is significantly different. Conventional cameras have the capacity to capture and store moving video, but it must first be downloaded before it can be viewed and analyzed; And this can only be done when the need arises.

In contrast, video captured by new technology is directly sent to a central surveillance center (the so-called "Lower Manhattan Security Coordination Center") where it is monitored and analyzed by a team of counter-terrorism specialists. According to the New York Police Department (NYPD), this Center, which opened in October 2008, is staffed by police officers of the NYPD Counterterrorism Bureau, but also includes staff from the private center.

However, addition to involving the local police, the new cameras can also transmit data in real time to federal agencies in Washington, including the Department of Homeland Security and the Federal Bureau of Investigation (FBI). It appears, therefore, that the New York surveillance system is, or will be, a component of the Total Information Awareness (TIA) network, which can integrate the transmitted videos with all other federal databases including the FBI's biometric database, which includes fingerprints, DNA samples, iris patterns, face-shape data, scars, tattoos, and unique mannerisms, such as the way people talk and walk.

The writer further points out that there are two questions that cannot rationally be avoided. (i) How effective such a surveillance system is likely to be in averting future terrorist attack? (ii) And, is whatever protection that might be afforded by this system worth the sacrifice of privacy?

System such as the New York surveillance networks will have the capacity to learn the daily behavioural activities of average citizens, capturing them on camera - anything from someone going to the bathroom to a closet gay person having a "clandestine" rendezvous with his or her lover. Indeed, no matter how open a person may be about his or her personal life, everyone has secret, private things that he or she does not want monitored by state authorities. As Jim Harper, the Cato Institute Director of Information Planning, states,

"When law abiding citizens go out in public and move around, they don't expect to use new high-tech surveillance technology in order to track us and monitor us, extracting untold information in the process."

When such mass, warrantless surveillance also occurs in private (non-public) zones, such as where one lives or works, the invasion of privacy is unequivocally unlawful; for while one cannot (legally) insist on privacy on a public thoroughfare, this is not the case when the invasion of privacy occurs in a private facility. And, while it may be contended that one tacitly consents to such surveillance when one uses this facility, even this lame argument unravels when surveillance cameras become ubiquitous and cannot reasonably be avoided. Unfortunately, once the boundaries between public and private domains have been breached, there are no constitutional constraints left to stop the invasive progression.

Giving police and/or federal authorities the power to monitor law-abiding citizens in the course of their daily activities portends serious potential for abuse. In chapter six, it was seen how surveillance of electronic communications for the official purpose of searching out terrorists morphed into also monitoring journalists and media organizations; and how government's handling of the programme of embedded reporters led to censorship, even to the point of using a public relations firm to screen out journalists who disagreed with the government's war policy. These and other myriad other instances of government abuse suggest untoward potential for abuse in the case of systematic video camera monitoring of citizens.

For example, the system might be used to target anti-war demonstration exercising their right to peaceful assembly, and perhaps follow around individual members. Technologies can also be attached to surveillance cameras that can capture citizens in private areas that would otherwise not be visible to other humans.

Chapter XIV refers to topic titled-**Beyond 1984: New Frontiers of Mass Surveillance**, in which the writer says that surveillance cameras have finite ranges within which they can track a person. However, there are other technologies that can be used to track people in real time, which are not constrained by location.

While talking about **Cell Phone Surveillance**, the writer says that one such technology in the common cell phone. In February 2010, following a lead from the Bush administration, the Obama Justice Department argued against in favour of warrantless tracking of cell phones. Regarding a case before a US appeals court, it held, "An individual has no Fourth Amendment-protected privacy interest in business records, such as cell-site usage information, that are kept, maintained and used by a cell phone company." If so, then the government can follow anyone about, from place to place, without a warrant. Thus, not only can the content of our electronic messages and Internet activities be monitored, our physical location can also be tracked in real time.

In fact, the precedent for government to track our physical locations through our cell phones was set as early as 1994 with passage of the Communications Assistance for Law Enforcement Act under the Clinton administration. According to Section 103 ("Assistance Capability Requirements") of this Act, telecommunication carriers are required to ensure that their equipment, facilities, and services are capable of supporting government surveillance in the provision of "call-identifying information", such as the origin, direction, destination, and termination of each communication generated or received by a subscriber. And it required that telecommunication carriers ensure that they have the capability of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier." Unfortunately, in contravention of the Fourth Amendment, the FBI has exploited such capability to conduct surveillance of individuals without warrant or probable cause.

In the chapter **Reality and the Politics of Power**, the writer, while giving the example of students' protest at Tiananmen Square in China on June 4, 1987, and its subsequent suppression by People's Liberation Army of China in which thousands of students were killed, says that the Chinese government refused to admit that the massacre even occurred. He says that the event is not mentioned in Chinese text books; Internet police patrol the Internet and block access to information about the massacre; Chinese media, which are State run, are forbidden from reporting about it; and the government arrests dissidents who attempt to speak out against what really happened, thereby indicating that in a culture of control (of which Communist China is an example), the government and its main stream media accomplices have power over what passes as reality. He says that in such a culture, it is not facts but rather politics that defines reality.

The writer further says that the possibilities for state-control reality are likely to increase with new technologies. In such a world, those who control the VR technologies will, like Orwell's Party, hold mastery over "reality" while the rest of us will be manipulated like puppets.

The idea of the state keeping its citizens focused on a make-believe world while they are exploited for purposes of world domination is not at all far-fetched. In fact, this has already happened, albeit in the low-tech world of cable and network news. For example, the American public has been the target of information and media warfare and "perception management" aimed at selling the war in Iraq.

This programme consisted of mainstream media dissemination of phony intelligence claiming that Saddam Hussein possessed weapons of mass destruction. It capitalized off of the 9/11 attacks by falsely linking Hussein to these attacks. It staged phony events such as the toppling of the statute of Hussein in Baghdad (staged by American troops, not Iraqi citizens) to symbolize an American victory; and a moral-boosting, heroic tale of the capture and escape of Private Jessica Lynch from an Iraqi hospital, which turned out to be a PR stunt, compliments once again of the Rendon Group. This was not virtual reality; nor was it reality. But, for the average American, it seemed real.

Building such bogus public perception may become an easier task with the advent of new delivery technologies. In fact, new digital technologies go beyond virtual reality to include "augmented reality", which is a hybrid between offline reality and virtual reality. Recently Lockheed Martin received a contract from DARPA to develop a set of lenses that would be capable of augmenting real objects with virtual images as well as data. For example, a soldier wearing these lenses would be able to mark an object with a number and other soldiers wearing these lenses would also be able to see the number superimposed on the object.

If such technology becomes mainstream, just how reality is transfigured will depend on who is behind the controls. Matrix-like worlds are in the offing. In the hands of a megalomanical government, "information warfare" and "perception management" can take on new and chilling meanings.

**The writer further says that technology is a factor in this degenerative trend but that is because of an underlying voracious appetite for money and power. What giant companies publish as news and information is largely determined by their bottom lines; and what governments enact as law is largely determined by corporate lobbies, politico-corporate quid quo pro, campaign finances, and the desire to stay in office. These politico-corporate factors tend to shape the reality that Americans see and hear on network and cable news shows.**

Further while talking about **Surveillance Video Cameras in the Classroom**, the writer points out that the attempt to control curricula at institutions of higher education becomes more disconcerting when it is coupled with a growing trend to install surveillance video cameras on college campuses. Allegedly for security purposes, at some universities, cameras have been installed in classrooms, which can monitor in real time professors' lectures and class discussions. This means that university administrators can legally monitor students and faculty without their knowledge or consent.

As bastions of democracy, colleges and universities are supposed to be free from abridgements of academic freedom; however, a consequence of such monitoring is to intimidate both students and faculty from freely expressing their views. The trend to install surveillance cameras, especially in classrooms, therefore threatens to undermine the culture of autonomy existing on college campuses and to morph this democratic forum into a burgeoning culture of control.

An increasing number of public elementary and high schools in the United states and Great Britain are also being fitted with surveillance cameras, allegedly for security purposes. Moreover, some cameras have also been purchased with federal money ( such as ones in Canton, Mississippi), raising the specter of federal monitoring of students' activities.

As a rule, state laws do not regulate the use of surveillance cameras in schools, hence increasing the possibility that surveillance cameras will be used for purposes other than maintaining security. However, some states have attempted to address at least some aspects of the lack of regulation. For instance, in 2009, legislation was introduced in the state of Washington requiring that notice be posted outside public school rooms and buildings stating that occupants may be subject to video monitoring. Unfortunately, such a proposal fails to address the more fundamental issue of purposes of monitoring.

If the FISA amendments are to serve as a model for prospective laws governing monitoring of students inside

their schools, then the "significant purpose" of such monitoring for purposes unrelated to this purpose. And as with FISA, unless there are provisions made for oversight - such as monitoring the monitors - it is unlikely that such laws will safeguard against abuse of information gleaned from classroom surveillance, for example, the firing of instructors based on their political views.

It was seen how surveillance cameras with interfaces to federal agencies have already been installed in private as well as public zones of major cities in the United States and Britain. It is, therefore, not surprising that such cameras are now starting to be used in schools. A logical step in this movement toward a culture of control is to attach school surveillance cameras to the massive total information network infrastructure already being operated by the federal government. If and when this happens, there is the real and serious possibility that education in the US will become little more than state indoctrination, monitored and controlled by federal agencies.

The writer says that unless the trend to use surveillance cameras in schools is stopped, it can reasonably be predicted that this will continue to expand. In fact, in one recent case, without knowledge or consent of its students, a school district in Philadelphia had allegedly gone so far as to install software in school-issued laptops, which permitted school officials to remotely activate the computers' webcams and to spy on the students in their homes. The school district allegedly claimed that it had installed the software in the computers for purposes of recovering lost or stolen computers. However, at the time of this writing, a federal class action lawsuit against the school district is pending, which in part argues that, pursuant to the Fourth Amendment, the students' reasonable expectation of privacy with respect to the use of such computers had been violated. The outcome of this legal case will set a major precedent. If the right to privacy is permitted to be overridden for such purposes as keeping track of school equipment, then this will be tantamount to having no reasonable expectations about privacy, even in one's own home.

The writer further talks about **Common Confusions about Freedom and Democracy**. He says that the definition of "a free nation" has somehow morphed into the idea of a "free market", albeit one that is controlled by just a few behemoth corporations.

Having built a corporate dynasty on slave labor and the stifling of fare competition, retail giants, such as Walmart, have become the symbol of the free world, and many Americans have supported this new symbolism by becoming faithful patrons. Thus, many Walmart shoppers neither know nor seem to care about the expense paid in human freedom for this monolithic shoppers' paradise. Some may be too distracted by the savings and the wide array of products displayed on the shelves of a "superstore" to contemplate the gruesome reality behind it all.

In America, colossal health insurance and pharmaceutical companies reap large profits while millions go without adequate health care. Still, many Americans condemn "socialized" medicine because any such social constraints would mean the end of a free-market economy. The "logic" here is black or white. We can be socialists or capitalists (but not both). Since we are capitalists, we must reject socialism. This is precisely the kind of thinking that usurped the possibility of a public option in the recent attempt by the Obama administration to pass healthcare reform.

The consequence of accepting this line of thinking is acquiescence in a politico-corporate system that is markedly antidemocratic, exploitative, and unjust. Instead of condemning this system, many who accept it do so because they think it would be un-American (socialistic, communistic, and even fascistic) to oppose it. Thus, in the name of freedom, they embrace a free-market economy that is anything but free.

**The Intensification of Surveillance Crime, Terrorism and Warfare in the information Age**

Edited by:

Kristie Ball and
Frank Webster

Published by:

Pluto Press, London

## Bird's Eye View

Never before our public and private lives have been under surveillance as today. Whether we are shopping with a credit card, walking down the street or emailing a colleague at work, our activities are being constantly monitored. Surveillance has become more routine, more integrated and more intrusive.

Since September 11th 2001 surveillance has intensified further. Yet although individuals, groups, governments and states are more closely monitored, our security is not assured.

The contributors to this book explore the vast range of issues related to increased surveillance. What is going on in an area clouded by secrecy from the state and complacent reassurances from corporations? How do we track suspects and combat crime without also eroding our civil liberties and sacrificing our rights to privacy?

Focusing on these and other issues such as paedophilia, money-laundering, information warfare, cybercrime, and related legislation, this book spotlights benefits and costs of surveillance, and suggests how it is likely to develop in the future. The book has eight chapters.

Under the chapter 'The Intensification of Surveillance', the writers say that the surveillance involves the observation, recording and categorization of information about people, processes and institutions. It calls for the collection of information, its storage, examination and - as a rule - its transmission. It is a distinguishing feature of modernity. They further say that over the years surveillance has become increasingly systematic and embedded in everyday life, particularly as state agencies and corporations have strengthened and consolidated their positions. More and more we are surveilled in quite routine activities like making telephone calls, paying by debit card, walking into a store and into the path of security cameras or entering a library through electronic turnstiles. In recent decades, aided by innovation and information and communication technologies (ICTS), surveillance has expanded and deepened its reach enormously. Indeed, it is now conducted at unprecedented intensive and extensive levels while it is vastly more organized and technology based than till now. The writers further say that surveillance is a matter of such routine that generally it escapes out notice - who, for instance, reflects much on the traces they leave on the super market checkout, and who worries about the tracking their credit card transactions allow? Most of the time we do not even bother to notice the surveillance made possible by generation of what has been called transactional information (Burnham, 1983) meaning the records we create incidentally in everyday activities such as using the telephone, logging on Internet, or signing a debit card bill. Moreover, different sorts of surveillance are increasingly melded such that records collected for one purpose may be accessed and analyzed for quite another. For example, the golf club membership list may be attractive data base for the insurance agent or address list of subscriber to particular magazine may be especially revealing when combined with other information on consumer preferences. Such personal data are now routinely abstracted from individuals through economic transactions, and our interaction with communications net-work, and the data are circulated, as data flows, between various data bases via 'information super high ways'.

The writes say that it is this intensification of surveillance that is the subject of this book. They further say we concentrate our attention on the aligned surveillance surrounding crime, terrorism and information warfare. Though there are vital differences between these realms but developments have led to certain blurring at the edges.

According to the writers, surveillance of crime can involve anything from

observation of rowdy behavior in the street to searching bank accounts for traces of illicit financial movements. Meanwhile the pursuit of terrorist may call for anything from assiduous examination of airline bookings, identifications of hackers, to satellite monitoring of shipping thought to be ferrying weaponry. And information warfare calls for nothing less than continuous and all-seeing observation of real and putative enemies - where terrorists are major targets and where criminal activity readily becomes pertinent - using the most sophisticated technologies available.

The writers have particular concerns with the period since September 11, 2001. They say that the distraction by terrorists of the Twin Towers in New York City has stimulated, and perhaps even more importantly, legitimated, the acceleration and expansion of surveillance trends. In their view, it has also helped promote especially acute disciplinary forms of surveillance and has blurred still more already fuzzy boundaries between crime, terrorism and contemporary warfare. They say that certainly crime and terrorism have long being of major interest to surveillance agencies, but today we are witnessing a steep change whereby there is a massive increase in surveillance, an expansion of those deemed deserving of scrutiny, and integration of this with warfare itself. In this context, the Pentagon announced late in 2002 the 'Terrorism Information Awareness (TIA)' project. The project was developed as a response to September 11 and the consequent American priority of targeting terrorist threats (Goldenberg, 2002), which are now regarded as the major concern of the advanced societies' military.

The writer says that at the heart of TIA is the conviction that, by searching a vast range of databases, it will be possible to identify terrorists, even before they can strike. TIA will draw together the results of already prodigious surveillance activities in hopes that defence agencies will prove capable of spotting enemies before they cause mayhem. The premise is that, if everything can be seen, all obstacles and threats might be extinguished, and stability thereby assured.

And who, post 9/11, might there be object this? There are undeniable serious terrorist threats posed to citizens, and it is surely right that all measures possible are taken against those who would perpetrate such crimes. Our main concern here would not be to resist TIA outright, but rather to draw attention to the mammoth amount of surveillance that already takes place and which is the foundation on which TIA builds.

Nevertheless, it is worth observing that, if the scale and scope of TIA is awesome, it is neither unprecedented nor is its motivating spirit new (Bam ford, 2001). We would go even further: the thinking behind TIA expresses what might be conceived of as a compulsion to surveillance, which is endemic in the modern world, where order and control are the requisites of all else.

**Why Intensify Surveillance?**

The writers say that given that new surveillance-based practices emerge at regular intervals, various explanations for the spread of surveillance have been offered. None of them, it might be emphasized, give much credit to particular events, however cataclysmic these might be. They further say that our central contention would be that 9/11 encouraged an alignment of actors, organizations, debates and viewpoints, from different policy and academic spheres, all of which featured surveillance as a germane issue. Accordingly, national security was constructed as relevant to public and private sector positions on CCTV and crime control, Internet security, and consumer monitoring, with privacy issues temporarily taking a back seat. Indeed, Dennis (1999) reports that 70 per cent of Britons are happy to let companies use their personal data, on the condition that they receive something back, such as a personal service or other benefits. The attack on the Twin Towers has accelerated surveillance, but its steady progress was well developed before then.

The writers say that there is another explanation of surveillance, one that accounts for its spread in terms of it being essential to living the way we do. From this point of view everything that we do entails an element of surveillance. Such surveillance is at once personal (we look around ourselves, as well as inside at our own biographies, to ascertain what it is that we will respond to) and involves the garnering of information from others' surveillance (for example, we look more or less interestedly at reports of family breakdowns studied by experts to understand better our own circumstances and how we might most appropriately act). In this way, surveillance is an essential ingredient of what has been called the 'reflexive self', one considerably more self-conscious and capable of creating itself than its predecessors (Giddens, 1991).

Moreover, surveillance is now a requisite of our participating in today's world, since it is surveillance that enables individual choices and a genuine sense of self-violation. For instance, telephone networks routinely track every call that is made as an essential element of their operations. Much the same case may be made for credit and debit cards: they simultaneously surveille and thereby intrude into the individuals' private life and allowed those with access remarkable advantages in terms of day to day actions (for instance, no need for cash, foreign currencies, and so on).

The writers further say that it is important to recognize this paradoxical character of surveillance since it intrudes and enables at one and the same time. There is similar ambivalence about surveillance when it is seen from the perspective of social inclusion and exclusion. To be included as a citizen in our society one must submit to surveilled (for example, providing an address to the authorities, filing a tax return when required, submitting the records of one's health details etc etc), but in return one get access to range of desirable services (like, the vote, welfare rights, medical benefits….). Against this, one might endeavour to escape surveillance, but then he/she might be inviting both hardship and the attention of the disciplinary agencies. To say bluntly, to be included one must submit to surveillance, while the excluded will be watched willy-nilly.

The writers point out that there certainly are many well-rehearsed objections to the growth of surveillance. Prominent among them is a perceived threat to civil liberties. Many commentators are concerned that information may be accumulated for nebulous ends, or by the wrong people, or that the files will remain active even when they become long outdated. Secondly, there is also objection to surveillance on grounds of intrusions on privacy (e.g. Rosen, 2000; Garfinkel, 2000; Thompson, 1980).

The writers argue that the issue of privacy always - and rightly -- looms large in considerations of surveillance. They point out that Fischer-Hubner (2001) distinguishes three main areas of privacy-territorial, personal (of the body) and informational (of information about oneself). In Europe, privacy rights have been enshrined in the Human Rights Act (1998). On the other hand, Tunick (2000) raises the question whether expectations of privacy are reasonable in the face of the new technologies of surveillance that appear in our everyday life. He suggests that privacy can be violated if our right to disclose autonomously information about ourselves is removed. He says the same applies to a personal e-mail and to a personal dairy if both were read without authorization. But the fact is that some degree of surveillance is a requirement of contemporary ways of life. In consequence, the key issues revolve around the character and motivation of the surveillance (what categories of surveillance are mobilized and to what end?) and the point at which proper boundaries are to be drawn. These are questions properly asked and addressed by citizens as well as by politicians lawyers.

In the chapter **Surveillance after September 11, 2001**, the writer Davit Lyon points out that the September 11, 2001 terrorist attacks on New York and Washington prompted a series of responses, from military retaliation on the country harbouring Osama bin Laden to extensive anti-terrorist legislation aimed at domestic protection. Among the latter, one of the most prominent ongoing reactions was to enhance surveillance operations on a number of fronts and there has been no lack of proposals concerning to best way to achieve this.

The writer raises the question as to what aspects of social structure and process may be seen through the prism of surveillance responses to September 11? He suggests that prism helps to sharpen our focus on two matters in particular: one, the expansion of an already existing range of surveillance processes and practices that circumscribe and help to shape our social existence; two, the tendency to rely on technological enhancements to surveillance systems (even when it is unclear that they work or that they address the problem they are established to answer.

The visible signs of putative changes in surveillance have both legal and technical aspects. The US and several other countries have passed legislation intended to tighten security, to give police and intelligence services greater powers, and to permit faster political responses to terrorist attacks (New York Times, 2001b).

**Several countries have proposed new national identification card systems, some involving biometric devices or programmable chips; others have brought forward more limited ID card systems, such as the new Canadian Immigration Card or the 'smart ID' for asylum seekers in the UK (Toronto Star,2001; Guardian, 2001).**

**In some respects bound up with legal issues, and in others, independently, 'technical' responses to September 11 have also proliferated. High-tech companies, waiting in the wings for the opportunity to launch their products, saw September 11 providing just the platform they needed. Not surprisingly, almost all the 'experts' on whom the media called for comment were representatives of companies. Thus, for instance, Michael G. Cherkasky, president of s security firm, Kroll, suggested that 'every American could be given a: "smart card" so, as they go into an airport or anywhere, we know exactly who they are' (New York Times, 2001a). Or in a celebrated case, Larry Ellison (n.d.), president of the Silicon Valley company Oracle, offered the US government free smart card software for a national ID system. What a commercial coup that would have been! He failed to explain, of course, what price would be charged for each access to the Oracle database, or the roll-out price tag on a national smart card identifier.**

Other technical surveillance-related responses to September 11 include iris scans at air ports - now installed at Schipol, Amsterdam, and being implemented elsewhere in Europe and North America as well; CCTV cameras in

public places, enhanced if possible with facial recognition capacities such as the Mandrake system in Newham, south London; and DNA databanks to store genetic information capable of identifying known terrorists. Although given their potential for negative social consequences there is a lamentable lack of informed sociological comment on these far-reaching developments, where such analyses are available they suggest several things. One, these technologies may be tried but not tested. That is, it is clear that they work with the kind of precision that is requited and thus they may not achieve the ends intended. Two, they are likely to have unintended consequences, which include reinforcing forms of social division and exclusion within the countries where they are established.

A third and larger dimension of the technological aspect of surveillance practices is that seeking superior technologies appears as a primary goal. The kinds of technologies sought - iris scans, face recognition, smart cards, biometrics, DNA - rely heavily on the use of searchable databases, with the aim of anticipating, preempting and preventing acts of terrorism by isolating in advance potential perpetrators.

So, what do these post-September 11 surveillance developments mean, sociologically? Before that date, surveillance studies seemed to be moving away from more conventional concerns with a bureaucratic understanding of power relations (Dandekar, 1990) that in fact owes as much to George Orwell as to Max Weber. This puts a very high premium on seeing surveillance as a means to centralized power as exemplified in the fictional figure of Big Brother - the trope that still dominates many scholarly as well as popular treatments of the theme. Although some significant studies, especially those located in labour process arguments about workplace monitoring and supervision, see surveillance as class weapon (Braverman, 1980), this view is often supplemented with a more Foucauldian one in which the Panopticon plays a part.

A brief survey of surveillance study shows how the once-dominant model of centralized state international power has been challenged by socio-technical developments. The result is newer models that incorporate the growth of information and communication technologies in personal and population data processing, and more networked modes of social organization with their concomitant flexibility and departmental openness.

Here the writer asks - Is surveillance best thought of as centralized power or dispersed assemblage? He says the responses to September 11 are a stark reminder that for all its changing shape since World War II the Nation State is still a formidable force, especially when the apparently rhizomic shoots can be exploited for very specific purposes to tap into the data they carry.

With regards to the experience of surveillance it is worth asking - Is intrusion or exclusion the key motif? In societies that have undergone processes of steady privatization it is not surprising that surveillance is often viewed in individualistic terms as a potential threat to privacy, an intrusion in an intimate life, an invasion of the sacrosanct home, or as jeopardizing anonymity. While all these are understandable responses (and ones that invite their own theoretical and practical responses), none really touches one of the key aspects of contemporary surveillance: 'social sorting' (see Lyon, 2002a).

The experience of surveillance also raises the question - How far do subject collude with, negotiate, or resist practices that capture and process their personal data? Surveillance is not merely a matter of the gaze of the powerful, any more than it is technologically determined. Data-subjects interact with surveillance systems. As Foucault says, we are 'bearers of our own surveillance' but it must be stressed that this is not merely an unconscious process in which we are dupes. Because surveillance is always ambiguous - there are genuine benefits and plausible rationales as well as palpable disadvantages - the degree of collaboration with surveillance depends on a range of circumstances and attitudes. In the aftermath of September 11, it appears that anxious publics are willing to put up with many more intrusions, interceptions, delays and questions than was the case before, and this process is amplified by media polarizations of the 'choice' between 'liberty' and 'security'. The consequences of this complacency could be far-reaching.

Surveillance responses to September 11 are indeed a prism through which aspects of social structure and process may be observed. The prism helps to make visible the already existing vast range of surveillance practices and processes that touch everyday life in so-called informational societies. And it helps to check various easily made assumptions about surveillance - that it is more dispersed than centralized, that it is more intrusive than exclusionary, that data-subjects are dupes of the system, that it is technologically driven, that it contributes more to prevention than to investigation after the fact.

The writer says that for all its apparent weaknesses in a globalizing world, the Nation State is capable of quickly tightening its grip on internal control, using means that include the very items of commercial surveillance - phone calls, supermarket visits, and Internet surfing - that appear 'soft' and scarcely worthy of inclusion as 'surveillance'.

In the chapter **Data Mining and Surveillance in the Post-9/11 Environment**, the writer, Oscar H. Gandy says

thaat in his widely successful book on the future of cyberspace Lawrence Lessig (1999) suggested that the difference about surveillance in the computer age is to be seen in the ease with which the data generated from the routine monitoring of our behavior can be stored, and then searched at some point in the future.

Lessig and others who are concerned about threats to privacy (Lyon, 2001a) have identified the countless ways in which our behaviour in public places, as well as in the privacy of our homes, generates records that come to reside in the computers of corporations and government agencies.

Data mining is an applied statistical technique. The goal of any data mining exercise is the extraction of meaningful intelligence, or knowledge, from the patterns that emerge within a database after it has been cleaned, sorted and processed. The routines that are part of a data mining effort are in some ways similar to the methods that are used to extract precious minerals from the soil. However, the extraction of precious metals is often labour intensive, and represents risks to both workers and the environment, the extraction of intelligence from computer databases is increasingly automated in ways that reduce the direct risks to labour at the same time that they amplify the risks to society in general. Indeed, as I will argue, the impact of data mining on the social environment may, in the long run, ne more destructive than strip mining for coal.

Imagine if you can, the mountains of transactional data that are generated each time a consumer purchases commodities that have been marked with universal product codes (UPCs). When consumers use credit or cheque verification cards, or any of a number of retail vendors' discount cards, individually identifiable information is captured and linked with the details of those purchases. There is little wonder that large retail chains like Wal-Mart have been forced to invest substantial resources in the development of data warehouses to allow them to extract some of the hidden value in the terabits of data being generated each day throughout their expanding global networks (Gates, 1999, p.232).

While talking about **The Goals of Data Mining**, the writer says that in general, data mining efforts are directed towards the generation of rules for the classification of objects. These objects might be people who are assigned to particular classes or categories, such as 'that group of folks who tend to make impulse buys from those displays near the checkout counters at the supermarket'.

In the attempt to develop reliable sorting tools, data miners seek to discover patterns of association between demographic characteristics and a host of commercial behaviours. Discriminant analyses within the commercial sphere are often applied to the task of differentiating between high-value and low-value customers.

The writer says that the technology of data mining becomes more sophisticated with each passing day. Neural networks are just one of the more sophisticated analytical resources being used more widely in data mining applications. Neural nets are said to mimic the ways in which the human brain processes information. These systems learn, or become more accurate, over time. An experience-based learning model attaches and adjusts the weights that are applied to different attributes or variables in response to each correct and incorrect prediction or determination.

A number of firms have began to offer data mining services and software products that are supposed to make it easier for Web-based marketers to transform transaction-generated data into intelligence that can be used to facilitate customer segmentation. Well-defined segmentation schemes often become the primary resource of a marketing campaign. Among the leaders of this emerging market are firms with names like digiMine, Accrue, Netgenesis and Personify. These firms provide analytical services to Web-based companies.

The writer further says that there is an increased demand for data mining tools. He says while the firms that are providing the bulk of these data mining products and services will continue to try and shape consumer demand through aggressive marketing, they are also likely to realize something of a windfall in terms of the increased attention to the development and implementation of the data mining applications following the events of 9/11.

Less than a week after the assault on the Pentagon and the World Trade Center towers, an article in the business section of USA Today asked, 'What can tech companies do?' Jump-start the development and implementation of data mining techniques, was the unequivocal response. One executive from one of a handful of still-active Internet communications firms suggested that '[we] are experts at data mining and we have vast resources of data to mine. We have used it to target advertising. We can probably use it to identify suspicious activity or potential terrorists' (Maney, 2001, p. 613). This executive was probably referring to applications such as 'Online Preference Marketing' (OPM), through which an Internet user's browsing activities are classified into 'types of inferred interests or behaviours that may be attractive to advertisers' (Agreement, 2002, p.7). The primary change, of course, would be the development of indicators and categories that would be of interest to government offices charged with insuring 'homeland security' in the US (National Strategy, 2002).

Much more cautious responses were offered by other technology developers who suggested that we were probably still years away from the kinds of data mining technology that might have allowed us to predict and interrupt the plans of the hijackers (Maney, 2001). Nevertheless, in response to what they perceived to be a continuing threat of terrorism, the Pentagon announced a major initiative designed to speed the development of technologies that could actually be deployed in the 'war against terrorism' within 12-18 months (Streitfeld & Piller, 2002).

The writer says that at the top of the government's wish list was an appeal for 'ideas to identify and track down suspected terrorists and to predict their future behaviour'. This goal was linked with a desire to 'develop an integrated information base and a family of data mining tools and analysis aids'. What the Pentagon was looking for was an analytical resource that would assist in the 'identification of patterns, trends, and models of behavior of terrorist groups and individuals… . The system would allow "what if" type modeling of events and behavioural patterns and result in predictive analysis products.' Ideally, the Pentagon sought a system that could efficiently scan data in the nation's computer networks and if they 'discover that a member of an extremist group also bought explosives and visited a Web site about building demolition, they might be able to halt a potential attack' (France et al., 2001).

There are of course a great many reasons for being concerned about the sorts of dramatic changes in the ways in which the American government plans to escalate in the ways in which the citizens, their associates, and any visitors who might be defined as threats to the security of the 'homeland' under the broad powers granted under the USA PATRIOT ACT (Bowman, 2002). These concerns are multiplied in the face of evidence that the United States government has been able win compliance, if not active support, for its plan to increase the level of communications and data surveillance to be carried out on the citizens of other nations. Yet, there are, in my view, still more important concerns that are raised by visions of a tidal wave of commercial applications of data mining that will follow rapidly behind a Schumpeterian swarm of innovations (Preston, 2001) brought into being by this most recent activation of the military industrial complex.

The exchange of data mining applications between the government and commercial sectors is likely to be accelerated as a result of increase pressure and latitude for surveillance and data-sharing activities that have been approved under the extensive powers authorized by the USA PATRIOT ACT (2001). There is particular concern about the availability of details about individuals' searching of the Web (Bowman, 2002), in that the capture of URLs from public terminals and private computers provides easy access to the content of files accessed by individual users (FBI asks …, 2002; Government, Internet Industry, 2002; Madsen, 2001). Federal agencies are expected to increase their use of techniques that have become quite common within industry. In the view of one industry observer,

"As the blindfolds are removed, today's FBI agents will quickly discover a world rich in information, from public chat rooms on the Web to commercially available databases that focus on financial records to other databases that provide details on dubious public figures around the world and their known associates. … Perhaps one measure of success will be the day when among FBI agents there are more database experts than lawyers". ((Crovitz, 2002)

While talking about the **Social Implications of Data Mining**, the writer says that as I have suggested, data mining systems are designed to facilitate the identification and classification of individuals into distinct groups or segments. From the perspective of the commercial firm, and perhaps for the industry as a whole, we can understand the use of data mining as a discriminatory technology in the rational pursuit of profits. However, as member of societies organized under more egalitarian principles, we have come to the conclusion that even relatively efficient techniques may be banned or limited to the degree that they are accompanied by negative social consequences, or externalities.

In the chapter **The Constant State of Emergency: Surveillance after 9/11**, the writers David Wood, Eli Konvitz and Kirstie Ball say that the events of 9/11 accelerated trends and integrated various forces towards an intensification of surveillance in the Western world. They argued that the current situation has been progressively emerging throughout the twentieth century, with 9/11 being only one of a series of recent events that focus attention on surveillance as both a solution and the problem. In the preceding chapters, surveillance applications in areas of deviancy and security management, business practice, and law enforcement were examined. New occupational groups, technologies and organizations, from the public and private sector, and especially the media, have become more closely aligned under rubrics concerning national security, profits, and risk management, to intensify surveillance practice. At the same time conflicts and inconsistencies, and new possibilities for resistance, have also emerged.

The writers say that Oscar Gandy, in his examination of data mining, highlighted the ease with which data are now stored and searched via sophisticated statistical techniques, at low costs. The statistician now becomes an agent of surveillance, as has the new generation of data mining software products, which compete and defuse via the market. The same applies to digital cameras whose images can also be mined. The mainstream application of data-mining results in consumers, buying behavior being more stringently defined, and the most value-added and risk-free customers being 'cherry-picked' for the marketing of premium products. A more detailed category of person is being included and excluded from various domains of consumption.

Furthermore, they say companies that sell data mining technologies were some of the first to respond to the US government's appeal to find information about suspected terrorists. Modeling events based on the movements and transactions of suspected groups has become commonplace for data miners who use these tools in risk analysis and accident investigation. Given the integration of these technologies into a national security network, Gandy observes the significant privacy and human rights concerns that are associated with the virtual, rather than spatial, delineation of people, removing any strong basis of protest. Data mining, it seems, both extends and intensifies surveillance networks, and with privacy laws in his view having limited effect, mass media opinion, according to Gandy, is required to combat its spread.

Yet, the writer says that all is not lost. When Charles Raab, examined problems with the leveraging of privacy codes to protect widespread abuse of personal information in the context of UK government, fragmented picture emerged. To improve public services in the UK, public and private sector organizations have become more closely aligned, under a strategy called 'Information Age Government' (IAG) and are frequently reliant upon information technologies and data exchange to achieve this integration. With the immense potential for intensified surveillance of individual citizens via data-sharing, Raab questioned whether this alignment had been achieved in the first place, and examined the content and consistency of approaches to privacy used to protect personal data. Raab identified a 'ladder' of privacy concepts applied across different governmental organizations means that information-sharing is difficult to achieve, despite IAG's wholistic rubric. Illustrations from the National Criminal Intelligence Service (NCIS) and application of the Crime Discover Act show that the corollary (and downside) is that no unified approach to privacy is adopted either.

The final, and most important point for surveillance theorists in particular, highlighted in this book, is the scale and complexity of surveillance practice. Both UK and US governments have huge ambitions concerning the integration of personal informations of the population, electronically integrated government, and slick, blood-free (on their part), information-intense warfare. Despite this, the chapters have highlighted the tensions and conflicts, not just at the very local level, but also the organizational, inter-organizational, and inter-state levels of surveillance practice.

The writers further say that the complex interweaving processes that take place between the social and technical, and the civil and military, need to be far better theorized. This is particularly important if one is to take seriously Cary Marx's 'new surveillance' argument (Marx, 2002), and the assertion that it is technologies, particularly information technology, that have made the surveillance society possible. While surveillance has long been acknowledged to work in a network-like fashion (Foucault, 1979) few recent studies of surveillance have addressed it, either empirically or theoretically, in this fashion (Ball, 2002). In the context of modern, digital surveillance, the software development suits facilitate panopticism; scientists, engineers and programmers are involved in state, military and corporate networks and are key parts in the development and functioning of surveillance systems. These people make the decisions that affect the invisible programming of the systems in the market place; elsewhere, another individual reasoned that a fit of so many pixels was enough to identify a face in a biometric system. These invisible, but influential decisions, their influence, and diffusion are poorly documented in the surveillance literature.

In the end, the writers say that research should attempt to take the experiences of watched consumer, software developer, and the gated community into account, as well as the interests of organizations and states in protecting their interests, rather than their citizens, using surveillance-based techniques.

## State of Surveillance: Tripping Out on Technology and The Global Fight-Back

By:

Ben Hayes

Published by:

TNI in collaboration with OCCUPY.com

## Bird's Eye View

This 9-page chapter is part of the document 'State of Power 2014, Exposing the Davos Class'.

The content of the chapter can be gauged by following quotation of Edward Snowden given at the start of the chapter.

Even if you are not doing anything wrong you are being watched and recorded. You simply have to eventually fall under suspicion from somebody even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you have ever made, every friend you have ever discussed something with. And attack you on that basis to sort to derive suspicion from an innocent life and paint anyone in the context of a wrongdoer. (Edward Snowden, June 2013).

**The surveillance state laid bare**

The Writer says that in 2013, Edward Snowden revealed that the surveillance capabilities of some of the democratic governments of the West are such that they can access almost anything their citizens do online or over a fixed or mobile telephone in the absence of democratic and judicial controls.

The writer points out that these powers are most advanced in the USA-UK led "Five Eyes" alliance (which also including Australia, Canada and New Zealand) but many other European countries and NATO partners are known or believed to have advanced surveillance capabilities and to have cooperated closely with the NSA (the National Security Agency of the USA) and GCHQ (the UK Government Communications Headquarters).

What is new and important for the state of power is the simplicity with which individuals and entire population can be placed under surveillance, the pivotal role that private companies play in facilitating this surveillance.

In response to the revelations, newspaper editors and government whistle-blowers have joined more than 300 NGOs and 500 prominent authors from across the world in demanding an end to mass, indiscriminate surveillance.

**Key revelations**

The writer says that highlights of the NSA Files released so far include:

- The Verizon Court Order : the first of the Snowden leaks revealed that the NSA was collecting the phone records of millions of Americans.
- "PRISM" enables the NSA and GCHQ to "mine" information from the servers of some of the biggest American technology companies (Google, Apple, Microsoft, Facebook, AOL, PalTalk and Yahoo). A similar programme called "muscular" was intercepting millions of records a day from Yahoo and Google.
- "Tempora", part of the "master the internet" programme: GCHQ intercepts and stores the vast amounts of data flowing in and out of the UK via the undersea fiber optic cables. Similar "bulk-intercept" programmes are run by the NSA (Blarney, Fairview, Oakstar and Stormbrew).
- "Xkeyscore": an NSA run data-retrieval system used to access e-mails, telephone calls, internet usage records and documents transmitted over the internet.
- "Boundless informant": a data analysis and visualization system that provides an overview of the NSA's surveillance activities by country

or programme. Almost three billion "data elements" from inside the United States were reportedly captured by the NSA over a 30-day period ending in March 2013.

- "Bullrun" and "Edgehill": a $250 million-per-year programme under which the NSA and GCHQ (respectively) have defeated much of the encryption technology that underpins the security of the internet.
- Cyberwar, espionage and collusion: further revelations detail the extent to which the US is prepared to use international cyber-attack to "advance US objectives around the world", the monitoring of phone calls of 35 foreign leaders and the complicity in NSA-GCHQ surveillance of intelligence services of - among others - Belgium, Denmark, France, Italy, Japan, the Netherlands, Norway, Singapore, South Korea, Spain and Sweden.

**"By any means possible"**

The writer says that entire communication networks are being placed under surveillance, whether 'lawfully' under 'voluntary' cooperation arrangements (between spy agencies and the companies that own those networks), or through state sponsored "hacking".

The NSA has also been building "backdoors" into the applications and software of some of the world's largest IT companies and using malicious software to steal information from private, government and business networks. A recent document suggested that the NSA has "infected" more than 50,000 computer networks worldwide.

Together, the NSA and GCHQ have also compromised the cryptography that enables the transmission of information security across much of the internet. Tim Berners-Lee, inventor of the World Wide Web called their endeavours "appalling and foolish" because they would "benefit criminal hacker gangs and hostile states.

**"Big data", Bigger problems**

The writer says that the revolution in Information and Communications Technologies (ITCs) is transforming our relationship with everyone and everything. The more and more of our relationships move on line, more and more information about us is collected. Everything is recorded, stored and analysed. The economic and organizational rationale for keeping this data forever grows stronger every year. As more and more of the things we own are connected to the digital world, and more and more online services are provided for us, the more sensitive and complete the information we commit - where we were, what we did and who we did with. We leave this data everywhere. It includes personal data (information identifying us), content data (what we write and say), and "metadata".

The need to protect ourselves from intelligence and security agencies bent on circumventing our rights to privacy is thus only part of the problem. We also need to make sure we are protected from those companies whose bottom lines depend on accessing (and monetarizing) as much of our personal information as possible.

Achieving meaningful reforms that properly address this problem is a much more difficult proposition because of the vested interests in maintaining the status quo and the jurisdictional issues that arise in any attempt to restrict transnational surveillance networks. These problems are compounded by profound changes in the relationship between people, states and corporations.

**Silicon valley vs the NSA**

The writer points out that in December 2013, eight of Silicon Valley's most successful technology firms - Aol, Apple, Facebook, Google, Linkendin, Microsoft, Twitter, and Yahoo - called for "wide-scale changes" to US government surveillance based on five principles for reform: (i) "sensible limitation" on government collection of information and an end to bulk data collection, (ii) stronger oversight and accountability of intelligence agencies, (iii) transparency about government demands and surveillance powers, (iv) respect for the free flow of information and (v) a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions.

It is notable that fixed line and mobile telephony companies, many of which have been unquestioningly facilitating state surveillance for much longer than their web-based counterparts, have not weighed in to the debate in the same way; though they never claimed to be pro-democracy either.

The writer further says that nothing apparently stirred the White House into action more than the concern that the revelations had been particularly damaging for some of the USA's most valuable corporations. But it also begs broader questions about how corporate power is exercised. Some of these companies have been or become proactive in pushing back on state surveillance, but some of them have also been fiercely resistant to

draft legislation designed to give individuals greater control over what happens to the personal data that their profit margins depend on, including provisions with the draft EU Data Protection Regulation.

We will help protect you from government surveillance but you don't need protecting from us is quite a proposition for a group of companies who, according to Fobers, spent more than $35 million on lobbying activities last year.

There can be little doubt that these companies are genuinely opposed to the kind of dragnet surveillance and data warehousing being conducted by the NSA because it is a genuine threat to their bottom line.

**Europe vs the "Great Satan"?**

Public outrage at the Snowden revelations is such that there is now significant political capital bound up in surveillance reform.

The writer says that EU governments adopted a joint statement criticizing their Transatlantic partner and warning of a collapse in trust, but not threatened further sanction. Angela Markel, the German Chancellor, has done a great job of playing to the domestic crowd (NSA "like the Stasi", "friends don't spy on each other" etc) while largely ignoring widely held concerns about domestic surveillance and dispatching a team of negotiators to Washington in what looked primarily like an attempt to secure Germany's admission to the "Five eyes".

The French government described the NSA's practices as "totally unacceptable" before including provisions in the Defense Bill 2014 - 2019 that grant its own intelligence services expanded powers to record telephone conversations, access emails, location and other "metadata" - with no judicial oversight whatsoever. Meanwhile the UK government, whose spying on its "friends" of a far greater magnitude than anything the USA has managed, has been the most brazen in rejecting any criticism, describing GCHQ's critics as "airy-fairy" types and encouraging a witch hunt against the Guardian. This has seen Glenn Greenwald's partner detained at Heathrow airport under terrorism laws and a laptop owned by the newspaper destroyed with an angle-grinder under supervision of state agents. None of this bodes well for the state of democracy in that country.

The European government has just completed an inquiry into the surveillance of EU citizens by the NSA and their European counterparts, but in the absence of the power to compel witnesses to testify, has relied on journalists, campaigners and independent experts. Its draft recommendations, which are not binding on the EU, will likely include the suspension of several data sharing agreements with the USA until it provides reciprocal privacy and data protection rights, the development of an "EU cloud" and reform of European mass surveillance programme.

In USA, a Federal judge has just produced a preliminary ruling stating that the NSA's bulk phone record collection is likely to be in violation of the US constitution, also labeling the practice "indiscriminate", "arbitrary" and "almost-Orwellian". This sentiment was then echoed by a Presidential 'Review Group on Intelligence and Communication Technologies' whose 46 recommendations - if implemented in full - would at least lead to some significant curbs on the NSA's surveillance powers.

**International law vs (trans)national security**

The writer says that whether we live in the kind of world where the NSA and its allies can do whatever they want to the internet and the secrets it holds or whether we don't really come down to know much respect we have for the rule of law and the principle of universal human rights, in particular the right to privacy - a right on which many other rights depend.

Limits to 'domestic' spying powers are relatively straightforward on the context of national constitutions which should afford citizens clear rights to privacy and protections from undue interference from the state. What is much more problematic is that nationals of other countries - who do not usually enjoy the same rights of citizens - can easily be subject to surveillance by a foreign state.

This is crucial for two reasons. First, digital communications frequently pass through the territory or jurisdiction of foreign countries, particularly the USA, where the majority of the world's internet traffic is destined. This means if you are not a citizen of the USA, any constitutional right to privacy you might enjoy in your own country is likely all but worthless as you traverse large parts of the internet. Second, while the main protagonist in the NSA Files is of course the USA, that agency is at the centre of a still highly secretive and almost entirely unregulated transnational intelligence network with global reach. This is why, as Privacy International has undertaken, opening up the "Five Eyes" is a prerequisite to meaningful restriction of its powers.

Obama's review panel surprised some by recommending that the surveillance of non-US citizens be subject

to be stronger oversight and that their right to privacy be recognized, but it effectively ruled out judicial protection for the individual subjects of foreign surveillance and proposed a lower threshold of "reasonable belief" (rather than probable cause) for surveillance required in the interests of national security. Neither would persons outside the USA benefit from the proposed obligations on the NSA to minimize the data held on US citizens.

This is unlikely to satisfy European critics of the USA's practices or the likes of the Brazilian government, which is demanding that all foreign telecommunications service providers operating in Brazil host their servers in that country so that their citizen's data is only subject to Brazilian law.

Advocates of global governance should be crying out for international agreements that both limit surveillance and enshrine individual rights to privacy and due process, but it is currently inconceivable that states will accept any international treaty that seeks to limit their national security capacities. The "big data" corporations can also be counted on to resist any attempt to codify the right to privacy or data protection into international law. For all the talk of surveillance reform, it is notable that the Silicon Valley principles make no mention of whatsoever of individual rights, digital or otherwise.

**Needles vs haystacks**

The writer further says that Edward Snowden's revelations have already inspired a growing number of legal challenges and courts in Europe and USA are being asked to weigh the legitimacy of what has been revealed against legal requirements to respect human rights and due process. This is the latest incarnation of the decade-old debate about the need to balance "liberty" with "security" and the new practices introduced under the "war on terror". In the political arena, "liberty" has taken the form of a struggle against mass, indiscriminate surveillance and in favour of laws mandating surveillance only when necessary, targeted and proportionate.

The writer further says that the power struggle is between a 20th century set of liberal democratic checks and balances, grounded in Nation states and the regulation of investigatory powers, and a new transnational, pre-emptive and mass surveillance-based model that has developed in the 21st century. The difficulty in trying to make this new model respect traditional notions of probable cause and due process is that the many of the methods it uses are antithetical to these notions.

Post 9/11, risk management paradigm has spread throughout the "Homeland Security" apparatus to encompass everything from pre-emptive detention to secret blacklists and extrajudicial killings by drone strikes, fuelling state repression across the world and encouraging the targeting of anyone who challenges the "status quo".

Forced to defend their bulk data collection programmes for the first time, intelligence chiefs have repeated the same mantra over and over again: "we need the haystack to find the needle". Consequently it is argued that any push back on surveillance compromises national security. While this provides a convenient defence of mass surveillance, the reality is that police and intelligence service alike have long had access to the "haystack" on a case-by-case or even blanket basis; What Snowden has revealed is the construction of giant haystack comprised of as much historical data as possible that allows the NSA and its allies to literally rewind to what their citizens have been doing at given points in time.

Ultimately, the current needle/haystack debate hinges on how much if any data should be retained by the companies that hold or carry it for law enforcement and security purposes and the circumstances under which it can be accessed. Danger lies in the smoke and mirrors that could normalize what exists instead of scaling back what has been revealed.

**The state within the State we're in**

The writer says that near the top of the list of most post-Snowden demands for surveillance reform are better oversight and accountability of the intelligence services. But given the lack of political will to fundamentally appraise how liberal democracies have allowed their intelligence apparatuses to become so extraordinarily powerful and unaccountable, this is a huge task.

That is why campaigns for surveillance reform are up against and it is naïve to think that demands for surveillance accountability will naturally succeed where a decade of trying to hold the USA and its allies to account for their roles in extraordinary rendition, torture, secret detention, internment and war crimes under the "War on Terror" have met with such resistance (not to mention the criminal conduct that goes much further back than 9/11). Across Europe and North America in inquiry-after-inquiry, proceeding-after-proceeding, the law has frequently failed to provide redress as States have closed ranks and governments have adopted the default position of defending, ignoring or exonerating the actions of their intelligence and

security agencies. Why? Because their national security and foreign intelligence apparatuses are intimately involved in everything States do militarily and in good deal of their foreign and economic policies and interests.

The writer further says that many campaigners talk about surveillance as if it occurs in a vacuum, ignoring the staggering development of national security apparatuses, particularly since 9/11, their impact on "suspect communities" and their relationship to strategies to combat "radicalization" and "domestic extremism". Across the world the kinds of peaceful protest and civil disobedience that democrats profess to cherish in under attack like never before with those who (logically) advocate more peaceful direct action cast as "extremists", even "terrorists". The struggle against unchecked surveillance should be at the heart of struggles for social justice.

We might also ask how it is that neoliberalism has successfully captured so many public services through the rubric of waste and efficiency, while the High Priests of the Security States can spend countless billions on armies of contractors and facilities? It is because what is good for the security state is good for business, and vice versa.

For example, "Homeland Security", most of it centred in some way or another on mass surveillance techniques, is already a multi-billion dollar business. With it comes an increasing blurring of the boundaries between military force, national security and public order and the mania for everything from drones to "less lethal" weapons, crowd control technologies, mass surveillance applications, militarized border controls, and everything else on show at MILIPOL (the 18th "Worldwide exhibition of internal state security" in Paris).

It must be assumed that an already powerful surveillance industry will seek to fill any "security" void created by the democratic control of state surveillance. If we are serious about limiting surveillance, we need serious restrictions on state and private sector alike.

**Power and autonomy under digital capitalism - from rights to currency?**

The writer concludes that globalised, mass surveillance has emerged because the international agreements designed to prevent the emergence of authoritarian states in Europe in the wake of the World War II have failed to check the consolidation of precisely this kind of illegitimate power, particularly since the end of the Cold War. Bodies like the EU and UN, captured by corporations or small numbers of powerful states, have inadvertently accelerated these processes. The "big data" controllers have secured all the rights and all of the information. Privacy has become something you opt-in-to: by shunning some services and availing yourself of others. There is market for this kind of "security" too, it just does not yet enjoy the government support and public subsidies that the security industry gets.

## Surveillance Indian Help

By:

Sagnik Dutta

Published in:

Frontline

New Delhi, August 7, 2013

## Bird's Eye View

This article highlights the involvement of two major Indian telecom companies in assisting the US in carrying out its surveillance programmes.

It says that a series of Network Security Agreements (NSAs) entered into by various U.S. government departments with foreign communications infrastructure providers from 1999 to 2011 allowed the US access to a considerable amount of data flowing through the cables of these companies.

Reliance Communications Limited and the erstwhile Videsh Sanchar Limited (VSNL), which is now called Tata Communications Ltd, signed network security agreements with US government departments including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Department of Justice (DoJ),and the Department of the Treasury (DoT), in November 2007 and April 2005 respectively, in order to oblige them to share data carried out on their infrastructure and assist the US in surveillance programme.

Even as the storm set off by the whistle-blower Edward Snowden's revelations about the United States' elaborate electronic surveillance programme is raging, a set of documents accessed by Frontline highlights the involvement of two major Indian telecom companies in assisting the U.S. in carrying out the programmes.

A series of Network Security Agreements (NSAs) entered into by various U.S. government departments with foreign communications infrastructure providers from 1999 to 2011 allowed the U.S. access to a considerable amount of data flowing through the cables of these companies.

Reliance Communications Limited and the erstwhile Videsh Sanchar Nigam Limited (VSNL), which is now called Tata Communications Ltd, signed network security agreements with the U.S. in November 2007 and April 2005 respectively. The U.S. government departments that were party to this agreement include the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Department of Justice (DoJ), and the Department of the Treasury.

A close analysis of these agreements reflects an elaborate attempt to control and monitor the flow of information through physical infrastructure owned by these companies. A similar pattern is observed in the agreements in terms of the mechanisms that are put in place to not only control and monitor transactional and other information of subscribers, but also protect access to the same by foreign governments and even the management of the company. The agreements also attempt to control foreign ownership of telecom companies. This illustrates attempts by the U.S. to dominate the cyberspace.

These agreements have significant ramifications for cyber-security policy in India. A significant amount of Internet traffic across the world, including from India, flows through the U.S. Internet infrastructure. The existence of such agreements makes such data available to U.S. government departments. What is noticeable in these agreements is the degree to which foreign control of the telecom companies is monitored and curbed.

On July 22, The Hindu reported that National Security Adviser Shivshankar Menon, in an internal note, called for international cooperation to counter cyber attacks. The note reportedly mentioned that the security agencies of the U.S. and the United Kingdom were "extremely stingy" in sharing information.

**Reliance Communications'agreement**

The writer says that an agreement signed by Reliance Communications Limited

and its subsidiaries (Reliance Gateway Net Limited, Yipes Holdings Limited and FLAG Telecom Group Limited) with the DoJ and the DHS (referred to as USG parties) in November 2007 provides that the communications service providers will provide technical or other assistance upon lawful request to facilitate electronic surveillance relating to domestic communications infrastructure.

It is significant to note in this context that at the time of signing this agreement, Yipes catered to financial, legal, government, educational and health-care industries through a network of more than 22,000 route kilometres of optical fibre and associated equipment across 17 major U.S. metropolitan markets. The agreement also mentions that Yipes had points of presence (PoPs) in London, Tokyo and Hong Kong and was in the process of deploying additional PoPs in Frankfurt, Toronto and London. Reliance Communications completed its acquisition of Yipes in December 2007. The acquisition was announced in July.

The writer further points out that Article 2, the key section of the agreement, clearly outlines the obligations of the company regarding storage of information on domestic communications. Section 2.4 states that unless otherwise agreed to by the parties, Yipes shall store domestic communications, transactional data, subscriber information, billing records, domestic network and domestic network management information exclusively in the U.S. Article 2.5 of the agreement clearly puts an obligation on Yipes to share such information on request with the U.S. government authorities. On a request made by a government authority, Yipes will have to provide any information in its possession and such information shall be stored exclusively in the U.S.

The agreement envisages an elaborate security framework to guard zealously this information accessed by the service providers. It states that within 10 business days of the effective date, Yipes shall designate a security officer to act as a point of contact between the USG parties regarding compliance with this agreement. Article 3.1 of the agreement says that the security officer will have to be a resident U.S. citizen, hold a U.S. security clearance and possess the authority to enforce the agreement. The security officer is given considerable powers and access to information.

The agreement states that the security officer "shall have access to all information necessary to perform his or her duties, including, without limitation, security-related and technical information and business information, including but not limited to information regarding the existing and emerging products and services of Yipes and business plans of the communications service providers affecting Yipes' ability to perform its obligations under this agreement". It further states that if any action of the security officer is blocked or if he is denied relevant information, the officer shall immediately report the fact to the USG parties within five days of such an incident occurring.

Further, Article 3.10 of the agreement provides that Yipes, upon a request from the USG parties, shall provide the name, date of birth, and other relevant requested information of each person who regularly handles or deals with sensitive information. Also, the company is bound by the agreement not to disclose sensitive information to any third party, including those who serve in a supervisory, managerial or executive role with respect to the employees working with the information (Article 3.11).

Article 4 of the agreement outlines attempts to manage the structure of the company and exert considerable control over ownership by foreign entities. Article 4.2 of the agreement says that a member of the management of Yipes acquiring information about a foreign entity acquiring ownership in the company or the domestic communications infrastructure above 10 per cent shall notify Yipes in writing within 10 business days. Also, Article 4.3 of the agreement states that if any foreign government or foreign government-controlled entity participates in the management of the company in a way so as to interfere with Yipes performing the terms of the agreement, then a member of the management aware of such developments will notify the USG parties within 10 business days of the timing and nature of the foreign government's plans.

Article 4.7 allows the USG parties to visit any time any part of the domestic communications infrastructure and Yipes' security offices to conduct on-site reviews regarding the implementation of this agreement.

Article 7.3 of the agreement says that violation of any obligations of this agreement shall be considered irreparable injury and monetary relief will not be adequate remedy. The agreement states that the USG parties shall be entitled "to any remedy available to law or equity, to specific performance and injunctive or other equitable relief".

A detailed questionnaire addressed to Reliance Communications remained unanswered at the time of writing this report.

**AgreementwithVSNL**

The writer says that a similar agreement was signed between VSNL and the U.S. government departments

which also provided an elaborate framework of surveillance in collaboration with the telecom company. The agreement was signed by VSNL and its subsidiaries (VSNL America and VSNL Telecommunications (U.S.), or VSNL U.S.) with the DoJ, including the FBI and the DHS, and the Department of Defence, collectively referred to as the "Parties", between April 5 and 7, 2005. This was to be followed up by an agreement, dated July 25, among VSNL, VSNL Telecommunications (Bermuda) Ltd and Teleglobe International Holdings Ltd and affiliated entities to facilitate the filing of applications with the Federal Communications Commission (FCC) for authorisation to assign and transfer control of certain licences granted by the FCC. (VSNL acquired Teleglobe in July 2005.)

The agreement provides the U.S. government departments a mechanism for seamless and holistic access to information flowing through the physical infrastructure of VSNL and Teleglobe. Article 1.3 of the agreement says that VSNL shall ensure that all domestic telecommunications routed over the Teleglobe network shall not be routed outside of the U.S. and/or Canada except in emergency situations such as a natural disaster. The agreement also grants the U.S. government departments unimpeded access to information concerning technical matters and physical management or other security measures and the right to ensure compliance with its terms.

Article 2.1 states that all domestic communications infrastructure shall at all times be located in the U.S. and it shall pass through the facility of VSNL America or VSNL U.S. located in the U.S. from which electronic surveillance can be conducted. As per Article 2.3, these two entities are obliged to store domestic communications, wire or electronic communications, transactional data, subscriber information, billing records of customers who are U.S.-domiciled, and network management information.

This agreement also provides a similar elaborate security apparatus to enable electronic surveillance and access to sensitive information. Article 3.2 of the agreement states a security officer shall review visits by non-U.S. persons to any domestic communications infrastructure. A written request for approval of a visit was to be submitted to the security officer no less than seven days prior to the date of the proposed visit. Article 3.8 also talks about points of contact to be assigned to VSNL America and VSNL U.S. security offices who shall be available for 24 hours a day, seven days a week, and shall be responsible for maintaining the security of classified, sensitive and controlled unclassified information. The two companies are also obliged to comply with any request from the U.S. government authorities for a background check or a security clearance process to be completed for a designated point of contact. The U.S. government departments are also given considerable powers regarding the appointment and screening of security officers handling sensitive information.

The clauses of Article 3.14 clearly point to the degree of penetration that this agreement allows to the U.S. government departments. It states: "Upon request, VSNL America or VSNL U.S. shall provide to the investigation services of DHS, DOJ, FBI, and DOD, or in the alternative, to the investigation service of the United States office of Personnel Management ('OPM'), all the information it collects in its screening process of each candidate."

This agreement also states that the breach of the terms will entail "irreparable injury" (Article 4.3) caused to the U.S. government departments and they will have the right to any other remedy available at law, to "specific performance and injunctive or other equitable relief".

An e-mail questionnaire to Tata Communications about the agreement did not elicit any response at the time of writing this article.

The existence of these agreements highlights the concerted attempts by the U.S. government departments to appropriate global telecom infrastructure to establish dominance in the cyberspace.

**The involvement of two major Indian telecom companies in this elaborate framework of surveillance in collaboration with U.S. government departments has significant implications for cyber security policy in India. The larger question facing the advocates of Internet democracy and privacy in communication is whether the Indian telecommunications companies will be similarly appropriated by an overzealous Indian government to obtain information about unsuspecting citizens and eventually as an instrument to control and monitor forms of dissent both in the real and in the virtual world.**

Another article titled-**How NSA hacks the whole world**, written by Prabir Purakayastha and Rishab Bailey, and published in Frontline dated June 26, 2013, states that the NSA is building a new $2-billion facility in Utah, which will have the capacity to store and process data equivalent to one million DVDs for every man, woman and child on earth.

The article says that Edward Snowden, a former employee of Booz Allen Hamilton, a defence contractor in the United State, has blown the cover off the vast snooping empire that the US has built.

The article further says that The Guardian has published a report on one such programme, Boundless Informant, which showed that 97 billion pieces of intelligence were collected from around the globe in the month of March

2013 alone. US has not only tapped into the global telecom networks but also gained access to the data of nine global Internet giants - Google, Yahoo, Apple, Facebook, and four others.

Subsequently, The Guardian revealed that the NSA and the United Kingdom's Government Communications Headquarters (GCHQ) jointly spied on the G-20 summit held in London in 2009. This G-20 meeting was largely focussed on economic matters, and the spying of the delegations was to give the US and UK delegations a negotiating advantage by knowing -in real time - the positions of other delegations.

What has created particular concern in the US is that under the secretive Foreign Intelligence Surveillance Act (FISA) court orders, all the US telecom companies have given the NSA all the transaction records of their millions of subscribers. These transactional data, what is called metadata, are not the actual phone conversations but records of who talked to whom, from where and for how long. The outrage in the US has largely focussed on its citizens being subjected to NSA surveillance. That the US is hacking into all the communications of the rest of the world has barely entered this discourse. And that is what concern us that the other 95 per cent of the world who are not US citizens.

The US and its Anglo Saxon allies, the UK, Canada, Australia, New Zealand, had set up a programme called Echelon after Second World War for spying on the global telecommunications network. Echelon was investigated by the European Union (EU), which issued a report on its activities in 2001, particularly that of Echelon passing sensitive commercial information to help US and UK firms against their EU competitors. Though the three earlier NSA whistle-blowers, Thomas Drake, William Binney and J. Kirk Wiebe, have been saying for years that NSA collects huge swathes of data of US and non-US citizens, it is the kind of details and documents that Snowden has provided that has finally caught the world's attention.

**Nature of the surveillance**

The writers say that what the Echelon programme did earlier, has now been widened enormously by NSA. It is not about just telecom cables tapped and satellite communications being monitored.

Snowden slides show that global fibre optic network, by which a huge part of global traffic passes through US, has been trapped. One of Snowden's slides shows that there are three such taps - a tap off the coast of South America, one in the North of Africa and another in the Indian Ocean. The most discussed method of surveillance used by the NSA is tapping into the servers of global Internet companies. All the Silicon Valley giants mentioned in Snowden's slide have tried to say they are not providing the NSA direct access to their servers, while at the same time admitting that they are duty bound under US laws to provide the NSA any data it wants. While the domestic clients of the US have some protection, though weak under the US law, the rest of the world has none.

The writers also state that US laws protect its citizens under the Fourth Amendment, which prohibits illegal search and seizures. While the US agencies have other instruments to access their citizens' data, the two preferred instruments are the National Security Letters (NSL) and FISA orders. The NSL was expanded enormously after 9/11 - with enactment of the draconian Patriot Act in 2001 and the FISA Amendment Act in 2008. Issuing a NSL requires no judicial oversight and can be done by the US federal agency, Federal Bureau of Investigation (FBI), Homeland Security, Central Intelligence Agency (CIA), or NSA. All the informations regarding such a letter are under a gag order - the organization or person served with the letter cannot disclose that he or she has received such an order, or, indeed, the content of the order.

The FISA court, which is supposed to review all actions or requests for surveillance of the executive, virtually rubber-stamps all the requests it receives. Only 11 out of a total of 33,900 such surveillance requests have been denied by the FISA courts since 1980. The primary purpose of FISA was to protect US citizens from such abuse. After 9/11, the minimal checks and balances contained in the Act have been considerably weakened with various amendments to FISA.

**Surveillance of India**

The writers say that India is the most prominent targets of US intelligence gathering. According to The Guardian it occupies the fifth place among countries under surveillance, with 6.3 billion pieces of data, and ahead of China and Russia. The reason for this penetration is quite simple. Not only do Google, Yahoo!, and Microsoft (Hotmail) have a large number of Indian users, even government agencies and officials routinely use these web-based services for their communication. In February 2013, after the Hyderabad bomb blast, India's National Intelligence Agency (NIA) announced a reward of Rs. Ten lakh for information; the e-mail address for receiving such communications was a Gmail address. The NIA is either unaware that Gmail is fully accessible to the US intelligence agencies or it believes that it has nothing to hide from the US. Even the Prime Minister's Office and the Attorney General use such webmail services, as reported in Bloomberg Businessweek (July 18,2011). So do

many other Ministers, and even the Indian Air Force.

The writers further say that the same ignorance or callousness is being shown with regard to data relating to the Unique Identification Number (UID)/Adhaar. The UID Authority has selected three US companies-one for supporting and two for creating the data repository-without taking into consideration the fact that these US companies are duty bound to furnish their data if asked for by the US government ("Question for Mr. Nilekani" by S.G. Vombatkere, The Hindu, February 6,2013). The other issue is the complete lack of data security pertaining to information on government websites, networks and computers.

Worse, India is increasingly relying on US companies in the name of partnership with private sector as shown in the Joint Working Group for Cyber Security formed last year. All the countries , except US and UK, are affected by the US snooping.

The Federation of Indian Chambers of Commerce and Industry (FICCI) and the National Association of Software and Service Companies (NASSCOM), the two agencies who are partnering Indian Government's cyber security exercises, have AT&T, Microsoft, Google, Facebook. And Yahoo! As key members, who are now known to be partnering the US intelligence agencies. Similarly, the "Indian" team that the Ministry of Communications and Information Technology had constituted for the World Conference on Telecommunications in Dubai in 2012 had representatives from the same companies.

**How the Internet is governed**

**The writers say that today, Internet Corporation for Assigned Names and Numbers (ICANN), the key Internet body, functions under a licence from the US Department of Commerce. India, with certain other countries, had earlier called for a multilateral United Nations body to govern the Internet. The US opposed all such moves tooth and nail.**

They also say that attempts have also been made to bring certain aspects of the Internet, notably cyber security, under the International Telecom Union (ITU). Last year, the ITU placed some of these issues on the agenda of the World Conference on International Telecommunications (WCIT 2012) in Dubai, and the consequence was a veritable barrage of vilification launched against the ITU and its Director general. Civil Society organizations were told that this was a ploy by authoritarian regimes such as China, Iran and Saudi Arabia to suborn the freedoms on the Internet. A lobbying group was formed by leading US companies, including AT&T, Verizon, Microsoft, Googles and Facebook, and this group led the global charge against the ITU. Proposals from countries such as Saudi Arabia and Russia were withdrawn because such proposals could have affected the freedom of the Internet; but still the US and its allies walked out from WCTI, effectively preventing the emergence of any consensus. It is now clear that the issue before WCIT was not one of authoritarian regimes destroying the freedom of the Internet but that no limit should be placed on the US intelligence agencies' "right to hack the global Intrnet infrastructure.


**Infopack**

**Popular Information Centre**

peaceact@bol.net.in

peaceact@vsnl.com

Phone & Fax:

(011) 2685 8940

(011) 2696 8121



*FOR PRIVATE CIRCULATION ONLY*

*If Undelivered, please return to:*

**Infopack**

A-124/6 (2nd Floor), Katwaria Sarai, New Delhi 110 016

***Telefax : 26968121 & 26858940 # E-mail : peaceactdelhi@gmail.com & peaceact@vsnl.com***