Emergence of The Big Brother in 21st century

When Software Collides with
Politics, Economics and Society

BY SIDDHARTH MAHANUBHAV

Contents

Acronyms

Introduction

Part I:Bringing The Big Brother into Reality from the World of Fiction

Chapter 1: Is Orwellian Big Brother A Fictional Concept?

Chapter 2: Basis of Surveillance State in 21st Century

Chapter 3: Software and Surveillance

Chapter 4: The Big Brother : More than Surveillance State

Chapter 5: Thought Control in 21st Century – Algorithms/Software Manufactured Consent

Chapter 6: Open Standards, Open Protocols and The Big Brother

Chapter 7: Network Security, Encryption and The Big Brother

Chapter 8: Internet of Things (IoT): A Dream come true for The Big Brother

Chapter 9: The Curious Case of Cloud

Chapter 10: Centralization of Internet

Chapter 11: Looking into Hardware

Part II : Software and its interaction with Politics, Economics and Society

Chapter 12: Nature of Software

Chapter 13: Democracy, International Relations and Software

Chapter 14: Capitalism and Free/Open Software

Chapter 15: Software, Privacy and Trust

Chapter 16: Deep State and Software

Chapter 17: Developing World and Free/Open Software

Part III:Extra Topics

Chapter 18: Some General Solutions

Acknowledgements

References

Acronyms

TBB : The Big Brother

GNU : Gnu Not Unix

FSF : Free Software Foundation

EFF : Electronic Frontier Foundation

IPRs: Intellectual Property Rights

DMCA: Digital Millennium Copyright Act

IoT : Internet of Things

BCI : Brain Computer Interface

CCI : Competition Commission of India

HTTP: Hypertext Transfer Protocol

HTML: Hypertext Markup Language

XML : Extensible Markup Language

TCP : Transmission Protocol

IP : Internet Protocol

CSS : Cascading Style Sheets

W3C : World Wide Web Consortium

IETF : Internet Engineering Task Force

IEEE : Institute of Electrical and Electronics Engineers

DRM : Digital Rights Management

EME : Encrypted Media Extension

UN : United Nations

NSA : National Security Agency

IPV6 : Internet Protocol Version 6

WTO : World Trade Organization

WIPO : World Intellectual Property Organization

EVM : Electronic Voting Machine

EULA : End User License Agreement

DNT : Do Not Track

IAEA : International Atomic Energy Agency

NSG : Nuclear Suppliers Group

NPT : (Nuclear) Non-Proliferation Treaty

NAFTA : North American Free Trade Agreement

ASEAN : Association of Southeast Asian Nations

IMF: International Monetary Fund

BRICS: Brazil, Russia, India, China and South Africa

EU : European Union

INGO : International Non-Governmental Organization

ICBM : Intercontinental Ballistic Missile

DNS : Domain Name System

VPN : Virtual Private Network

ISP : Internet service provider

Introduction

When I started reading ‘1984’ written by George Orwell for the first time a decade ago, I wasn't impressed. I found the novel boring, and the concept of Big Brother dry and uninteresting. I dropped the book after reading few pages. I understood the concept, but most probably I was not able to grasp the political message behind the fictional setting, because for me, the setting was unreal and had no implications whatsoever in the real world. Few years down the road, my perception about the world started to change, as I started taking interest in politics, society, economy and their interplay with technology. As my understanding of the surrounding started to improve, I decided to read the novel again with a completely new mindset, and at that time I was not disappointed. I found, the concepts utilized in ‘1984’ were not only far ahead of their time, but also had deep implications in technologically advanced, highly interconnected world of 21st century.

Since last few years, many books have been coming regularly in the market discussing in detail how surveillance is being done with the help of technology. Moreover stories and news of increasing digital surveillance and invasion of privacy are becoming ubiquitous. Therefore, writing another book on how surveillance is being done in today’s world is not my intention. Being from Computer Science and Engineering background, I already knew how technology could be misused for keeping eye on the people, as a result news of increasing digital surveillance never surprised me. However all theses stories piqued my curiosity in understanding the basis of Orwellian Surveillance State as depicted in ‘1984’, and I started wondering whether such a state could come into existence in a democracy. Soon after, I found myself working on this topic. I have been open source and free software supporter since over a decade now, therefore my first intuition was naturally to look into the nature of software in order to understand today’s surveillance. Orwellian Surveillance state can’t come into existence without technology, and software is at the heart of technological revolution that we are experiencing. Software brings every non-living device to life, making it focal point of every kind of surveillance activity. However, after some time I realized that software is necessary but it can not form sufficient basis on its own. There are multiple factors revolving around it, which are also needed to be taken into account in order to understand the basis of surveillance state, about which I have tried to elaborate in the present work.

In this book, an attempt has been made to find out co-relation between software and the ecosystem surrounding it and the concept of Orwellian Big Brother. The book has been broadly divided into three parts. The first part mainly deals with finding out and understanding the basis of surveillance state in the 21st century. The second part deals with studying interaction of software with politics, economics and society, and finally the third part enumerates some measures which users can take at the present moment to protect themselves in this digital world.

The book is not against any particular corporation or organization. It just wants to start a wider discussion on the topic of freedom and transparency in software and the ecosystem surrounding it, so that people can take well informed decisions. Today technology armed with software is invading our lives. Almost every field that we can think of - from space research to farming - utilizes software in one form or other. Therefore it is increasingly becoming necessary to look into the nature of software and how it interacts with our lives and the institutions that we have built around ourselves.

I am not a gifted writer, and this is my first book. In addition to that, it has been written without any professional help. Therefore, it is possible to have presence of editing errors here and there. But I hope, these editing errors won’t come in the way of understanding the concepts presented in it. If this book manages to arouse people’s interest on the issues of freedom and transparency in software and the ecosystem surrounding it, then I’ll say that my task has been more than accomplished.

Siddharth Mahanubhav

Part I

Bringing The Big Brother into Reality from the World of Fiction

Chapter 1

Is Orwellian Big Brother a Fictional Concept?

Big Brother is a fictional character in George Orwell's dystopian literary masterpiece ‘1984’. In this novel he is portrayed as the dictator of the state of Oceania – a completely totalitarian and authoritative state which is controlling each and every aspect of its citizen's life. His real identity is never revealed. Whether he is dead or alive, no one knows. Citizens of this state think that he is kind of an immortal - who will never die. He is basically a symbol of political party, that is controlling the state, or we can say that he is the symbol of the state itself. In the novel it's always reminded to the citizens that ‘Big Brother is Watching You’ via electronic instruments such as ‘Telescreen’ - a fictional device combining features of TV and security camera. It means they are constantly under surveillance by the state. It's a constant reminder to them that they should not indulge in any anti-state activity. The state in the ‘1984’, is shown so powerful that it even controls thoughts of its citizens. If one has different ideology or belief system, then it won’t hesitate in utilizing coercive methods to alter one’s thought pattern; because controlling thoughts of the citizens - so that they should be in sync with the ideology of the state, is the best method to strengthen grip over the state polity. If the ideology of the government of the state and its fellow citizens matches, then there is no opposition to state’s rule, since in such method people themselves acquiesce in their own domination without any protest as if they are doing it out of their own free will. But reality is that they are forced to think in that way without they themselves knowing about it. This coercive way of thought control is so powerful that it altogether jumbles up person's own memory and hence his own personality.

It is normally believed that The Big Brother as shown in '1984' might surface in closed political setup characterized by authoritarian and totalitarian regime. In democracies that we see today (most of which follow mix of liberal democratic principles and socialism), The Big Brother is a purely hypothetical and imaginary concept, and considered as just a figment of imagination of hyperactive security conscious individuals.

In democracies we believe that The Big Brother doesn't have a chance to surface (even though in such political setup state plays important role either directly or indirectly). There are some genuine good reasons because of which we have so much trust in democratic political setup. In a big brotherly state, complete state control is required over each and every sphere of the society including media and mass communication. And in democracies, it is almost impossible to do so.

In democracies, we highly restrict the coercive power of the state via constitution. In this system, we choose our representatives via election that follows the principle of one person - one vote, there is a limit on the power a state can exercise and there is freedom of speech and expression. There are always rules and procedures that the state has to follow and it certainly can't act arbitrarily because it is bound by the constitution which is more or less a contract between state and its people. And breaching the contract means breaching the trust that people have on the state. If people feel that contract has been breached, then they elect another government by conducting free elections. There are certain rare situations like war or external aggression during which state acquires extraordinary powers which is known as emergency, but most of the constitutions impose certain limits under such conditions as well. Therefore it is general belief that democracies are immune to the concept of The Big Brother, and it is applicable more to the close political-economic systems and dictatorships. Because if people get to know that elected government is behaving like The Big Brother then they will elect another government through constitutional methods by conducting another election.

But advancements made by science and technology in the last 20-30 years have thrown very different kind of challenges to the democracies all over the world. We now think that due to revolution in Computer and Information Technology, it's almost impossible for the state to control public opinion and any kind of public dissent. We have examples like Arab Spring, whose spark was ignited by internet and social media, that completely changed the political landscape of Arab Countries. Therefore every country now takes internet very seriously, and many optimists believe that internet has ushered a new era in democracy, which will make democracy not only responsive but also participatory in nature. We started to believe that democracy is secure even more than before, as there is no way to curb public opinion or political dissent, due to decentralized and open nature of internet. However, at the same time, everyone failed to see the massive increase in surveillance capacity of the state due to all these technological changes.

Thanks to the Edward Snowden Episode, the surveillance scam came to the limelight. In spite of the episode, we haven't seen any drastic measures taken by government of any nation or any organization. After the Snowden episode there was just mud-slinging, blame game and shouting on one another. But no one took any concrete steps to find out any permanent solution. It seems that most of the people really don't know what to do; and even if those in power know what to do, they might not do anything about it. Everyone thinks that the state and its clandestine institutions are the real culprit. And if we somehow curb the arbitrary excesses of the state then we might be able to prevent it from becoming an ugly monster. But we fail to see some important structures of technology that constantly energize and give power to the state or any other agency for doing such work.

We want the state to be more open and transparent in every possible manner. In order to make working of the state more transparent, most of the democratic states have enacted acts like Right To Information - which allows any citizen of the state to request any information from the government. We know that such kind of acts are important to keep arbitrary and hidden activities of the state in check, because everyone knows that transparency is very important to ensure proper working of the state as per the constitution. Without transparency, we have no way of knowing what the state will do with it's immense power in hidden manner.

In the same way, there are some segments or we can say structures of technology, in which lack of transparency has created conditions, which can give tremendous hidden power to the state. But we don't want to change these structures which is fueling the hidden power of the state, because we are either unaware of such structures or we simply don't care about them or we are made to believe that such structures do not exist at all. In reality, such structures do exist and if we strike at this root itself, then state’s surveillance capacity will get a big setback. There are very few people and organizations who are actively engaged in bringing transparency in this structure, but most of the common populace is almost ignorant about it, due to its highly technical nature.

In the next few chapters we will try to explore various topics related to main structures that not only can enhance the hidden power of the state, but can also lead to creation of surveillance state in 21st century, which, if not contained within the limits of democratic setup, can transform into a full fledged Big Brotherly state, which will not only control all aspects of people's life, but will also bring one of the most intriguing concepts in fiction into reality.

Chapter 2

Basis of Surveillance State in 21st century

Developing basis of Surveillance State means determining the roots or factors on which such state can be based, by identifying its certain characteristics features. Once we know the basis, we can find out ways of preventing such state from coming into life in democracy, by reasoning out why the state might develop those features in the first place in the 21st century democracy.

There is no common agreement as to what constitutes a Surveillance State, hence we'll take the liberty in defining its core features.

Core Features of Surveillance State:

1. An Ability to keep close watch over almost the entire population of the state.

It's the general characteristic of any Surveillance State about which there is hardly any disagreement. Keeping close watch over citizens is not a new concept. State and its authorities are doing it since time immemorial on the ground of security. Earlier they used to keep watch over people of only suspicious behaviour, but today technology has opened avenues such that it's possible to keep track of each and every activity of each and every person.

2. Indirectness

Indirectness is another feature of Surveillance State. In democracy, people will certainly oppose any plan of direct mass surveillance by the state, with all the available legal, constitutional and democratic methods. Democracy allows surveillance within bounds of law and only within certain limits. Therefore, for creating Surveillance State, it is necessary to find out indirect ways of performing surveillance in a way that common people won't even have a clue about.

3. Complete disregard towards privacy of citizens

Surveillance requires disregarding privacy. Without violating privacy, it is impossible to keep watch over any person. If the state is violating privacy of a person or select few people and that too within bounds of law on the ground of security; then we won't say it is disregarding privacy. After all, a state has to protect its law abiding citizens from criminals and other threatful elements. But if it is violating privacy of a large section of population or almost the entire population, then it means that privacy is just a mere vocabulary in the dictionary of the state without any substance.

4. Heavy dependence on opaque technology

Surveillance especially mass surveillance can't be carried out without technology. And in order to carry out mass surveillance in an indirect manner, with complete disregard towards privacy, it is necessary to develop opaque technologies, which will carry out the work. We are surrounded by technology, and we have already developed technology which can do the work without human intervention. Hence, state or its organizations only have to find out correct combination of technologies, which will do the work in a clandestine manner unknown to every person.

After defining the core features, we will try to analyze factors which might help the state in achieving those in 21st century.

Keeping close watch over people in an indirect manner with a complete neglect towards privacy of citizens has never been easier in the entire history of humanity. We are all surrounded by electronic devices. Many of these devices, such as cell phones, are already laced with camera and voice recording functionality. Moreover, most of them are connected to the internet 24x7, and internet has become the most important source of information for people. So, all that is needed is to create an **opaqueness structure within devices and internet** which will help the state keep close watch over people in an indirect manner. Opaqueness structure here means hidden components of technology which will facilitate spying/surveillance or controlling people indirectly without people knowing about it.

Creating opaqueness structure within devices means developing technology which no one can audit, and whose implementation details remain unknown to general populace, so that people should get no idea that their devices are being controlled by someone else. Developing such a technology basically means developing closed software and hardware. Every electronic device is a combination of hardware and software. Hence by manipulating software and hardware, it is possible to manipulate any device. Closed software (or closed source software) is a computer program whose source code or programming instructions are neither published nor shared with common public for anyone to look at or change.[1] (Normally ‘closed software’ is referred as ‘closed source software’ or ‘proprietary software’, but in this book we will use the term ‘closed software’. All these terminologies will be discussed again in detailed manner, in ‘Part II’ of the book, in the chapter ‘Nature of Software’) Closed hardware means, hardware whose internal working and anatomical structure is kept hidden from general public. By using closed software and hardware combination, it is possible to fool public and keep a close watch over them, in a manner that no one could have imagined earlier.

However, software and hardware can’t remain closed unless they have a sound legal and institutional backing. Here legal and institutional backing means creating political, economic infrastructure - which typically takes the form of Intellectual Property Rights (IPRs), in order to protect software and hardware. IPRs are designed to protect ideas or forms of expressions, so that the creator can have exclusive rights over its own creation or product for a specific period. In order to protect both software and hardware, it is necessary to have strong intellectual property rights regime (IPRs), which will legally enforce the protection. But protection of both software and hardware won’t be of any use if other third parties have the choice to develop their own piece of software/hardware, that can provide same set of functionalities. For example, in most of the countries software is protected under copyright. Copyright protection means protection is granted only to a particular form of expression. As a result anyone is free to develop a software product that can provide functionalities similar to that of already existing software, but expressed in a different form. Therefore, traditional IPRs hardly look promising when it comes to protecting monopoly of a software product. So what should be done? The best way to solve the dilemma is to create a complete monopoly by developing closed proprietary standards, so that others won’t be able to create similar piece of software, which can provide the same set of functionalities but implemented in a different manner. (In this book a separate chapter - ‘*Open Standards, Open Protocols and The Big Brother*’ - has been devoted to discuss the issue of standards, hence if reader does not understand what closed standards means, then they should wait for few more chapters.) Closed standards are essentially required to maintain monopoly in a particular segment by breaking interoperability. It prevents others from entering the field. Therefore in electronic devices, closed software/hardware, rigid IPRs and closed standards form the unholy trinity which can help in creating opaqueness structure within it.

After devices, we will move over to internet. Internet can’t work without electronic devices or machines. Therefore opaqueness structure of devices will automatically become part of opaqueness structure of internet. But creating opaqueness structure in internet will require much wider strategy than that required for electronic devices. Internet is far more complicated, hence it is difficult to get any concrete idea about its opaqueness structure. But if we look at main purpose of internet, then we can get an idea about how opaqueness structure can be created within it. The main purpose of internet is to facilitate the flow of information. If someone or some organizations want to create opaqueness structure within it, then they just have to find out ways of controlling information appearing over internet. As number of people relying on internet for accessing information is increasing day-by-day, it is necessary for The Big Brother or the Surveillance State to control information appearing on it so that people can have access to only those pieces of information which they want people to see and not what people want to see. Information control is dependent on multiple factors, but prominent amongst them - which are necessary for creating opaqueness structure, are ability to gather and analyze infinite amount of data in an opaque manner, and a complete centralization of internet. Gathering and analyzing information over internet in an opaque manner is important for developing proper surveillance system. And controlling information over internet can become much smoother, if internet is completely centralized with some handful of organizations having control over it. Therefore, if we have to wind up in one sentence, then we can say that creating opaqueness structure within internet requires creating internet technology and services that can not only control flow of information but also have unlimited capacity of gobbling up data of every person connected to the internet without they themselves being aware of it, in a completely centralized manner with almost little control of people over their own information.

Now if we have to sum up briefly and list down the factors constituting the opaqueness structure in electronic devices and internet - which ultimately form the basis of surveillance state in 21st century democracy; then they can be summarized as follows:

1. Closed software/hardware.
2. Rigid Intellectual Property Rights Regime (IPRs).
3. Closed protocol and standards.
4. Controlling Flow of Information over internet.
5. Developing opaque internet technology and services that can gather and analyze data over internet anonymously.
6. Promoting Centralization of Internet.

We shall discuss all the factors mentioned above (with special emphasis on software), in various contexts, but not in any fix order, throughout the book, while discussing various aspects of Surveillance State or The Big Brother (TBB) in 21st century.

Chapter 3

Software and Surveillance

Software is at the heart of opaqueness structure which we've discussed in previous chapter, for it's lot easier to manipulate, and at the same time it's possible to hide what it's doing under the garb of IPRs. In the absence of software, computer or electro-mechanical devices will provide only limited set of functionalities, and especially in 21st century, they will be practically of no use without some or other kind of software. Now we'll take a look at some examples of software manipulation in real world by some corporate giants, which will make it clear as to how easy it's to adulterate software which then can be used for any kind of surveillance activity.

In 2005, SONY BMG copy protection rootkit scandal broke out.[1] In this scandal, one of the most respected and powerful companies of the music industry inserted some malicious rootkit via their CDs onto users' computers in the name of protecting digital rights of the music. A rootkit is a software or a collection of software that enables, an unauthorized user or an attacker to gain access to internal parts of the operating system, which, under normal circumstances are accessible only to root or administrator of the system. More often it masks its presence so that no one should get an idea that their system has been compromised. Hence, they are not only difficult to detect but also difficult to uninstall. Once it gets unauthorised access to the system, it's difficult to tell what it will do. Depending upon the intention of its creators, it can get complete control over the system and monitor every activity on it. By installing a rootkit, the company was trying to protect its own interests by directly taking control of user's computer.

It's a serious offence, because breaking into someone else's house without prior permission is certainly a criminal activity. Even though a computer can't be called as user's home, but it's an important component of our home and nowadays it is gaining distinction of being a virtual home. Once user's computer gets connected to the internet, it becomes a portal to the outside world. In other words, your computer acts as a door to your home from which anyone can get access to you and vice-versa. People won't get access to your home physically, but virtual access via internet is more than enough to know about yourself. Therefore, breaking into your virtual home without legal permission is certainly an offence. People might think that it might be the fault with the Windows Operating System or general lack of ethics on the part of the company SONY BMG, but there is something else that boosts confidence of such companies or crackers to perform such illegal behaviour.

In 2015, another scandal broke out involving another big company, but this time in the automobile sector. Volkswagen, a giant in the field of automobiles and the brand ambassador of German engineering and technology, cheated in emission standard.[2] It wanted to pass environment clearance test without following any emission standards. It cheated by rigging the proprietary software embedded in the car. Nowadays, most of the cars have software embedded into them for doing automated task, and most of the innovation in automobile industry is driven by software. The car software, which consists of millions of lines of code, performs variety of functions ranging from controlling brakes, door lock to adjusting speaker's volume. It is more efficient and cost effective than any mechanical control. As it is possible to write car software which can improve its efficiency and performance, it is also possible to write a car software that can easily fool the environment clearance test. And Volkswagen took advantage of that. It is much more cost effective for a company to rig the software for environment clearance, rather than creating a brand new car model with efficient engine and pollution control mechanism. The software embedded into the Volkswagen was created in such a way, that it turned on pollution control equipment only during inspection.[3] Once the inspection was over, the pollution control equipment would shut off automatically. It was really a smart but a very cunning solution to the problem of environmental clearance and green house gas emission. What exactly prompted the Volkswagen to do such a nasty thing? Profit motive and protecting its self-interest are certainly the main cause of doing this. But what is the inner structure that gave them confidence that they won't get caught red handed even after doing such unethical behaviour on their part? We can blame Volkswagen for its unethical business conduct, but there is some loophole in the technological structure itself that allowed them to use such dirty trick.

In both the above cases, the criminal activity is not important, but the way it has been done is something that we need to pay attention to, as it is not normal criminal activity but a very high profile one, that involves high level of technologically sophisticated knowledge. It involved altering the automated programming instructions, which forms the basis of modern electro-mechanical civilization. Why were they able to rig the software in the first place? Because the software was a closed one and heavily guarded by the strong IPR regime, which can't be audited by anyone except the company. Hence, they were sure about their cheating to be successful. We might feel that both the cases are nothing but corporate level frauds and we should not pay more attention to them than they require. But both these cases give indication of how hardware and closed software combination can easily fool the public. Just take a look around ourselves, and we will see that we are surrounded by all sorts of electro-mechanical devices which are embedded with closed software in them. Now just for fun try to list down all the gadgets around you that may contain software. Our computers or mobiles are not the only devices that contain software, but the whole range of electronic devices starting from TV, washing machines to refrigerator also contain automatic instructions in the form of closed software. Considering the software is not available for public scrutiny, just imagine, if a company or state agency wants to rig the software of these devices, can't they do it easily?

Whenever the word surveillance comes into picture, common people normally think about only modern electronic and communication equipments such as CCTV, satellites and variety of drones, and keep on believing that only such specialized devices made for surveillance are only capable of performing it, and we don't have to worry about it when we are out of their reach. But now we have reached a point where surveillance activity can become far deeper and can extend over the population of the entire world with the help of closed software.

We are all surrounded by electronic equipments such as TV, PC, mobiles, micro-wave ovens, refrigerator, washing-machines etc...in our homes and we can extend the list as much as we want to without any end in sight. As soon as we step outside the home, we encounter a number of vehicles ranging from bicycles to public transport vehicles. Currently good percentage of these vehicles have software embedded in them, but in future almost all the vehicles that we see on the road, will have some or other kind of software. Most of the public places are already laced with electronic surveillance equipment which are controlled with the help of some form of embedded software, which are then connected to a computer network so that someone else can control it remotely and supervise the locality from a distance.

We basically believe that all these electro-mechanical things are without any life and can do the things that we tell them to do. We feel that they don't possess any artificial intelligence (AI), because we feel that AI is something sci-fi terminology and we are far away from perfecting it, and that these things can't operate on their own. We feel that they need certain human assistance, hence there is no possibility of Terminator or Matrix like situation happening in our world. But once an equipment is programmed with the help of software, it can carry on its work without need of any external help. Therefore such type of intelligent behaviour of these devices should also be categorized as AI - but of low quality. And we have to understand that whenever a device acts on its own without any external interference, then it means it can be used as a very potent instrument for surveillance. There is no doubt that we are far away from developing a perfect AI as shown in the movies or in the science fiction novels, but we don't have to wait for a perfect AI - that can perfectly mimic human beings in every aspect, to see emergence of The Big Brother.

Closed software embedded into the device, which basically acts as its mind, can easily do the tasks automatically as per their default settings or on a given input/command. This AI is of very low quality and has limited utility, but it is more than enough to keep an eye on each and every individual. Hence we should not say that these electronic gadgets do not have any intelligence. In reality we are surrounded by such intelligent devices all around us, which means that we are surrounded by artificial intelligence 24x7. These gadgets certainly won't behave on their own owing to their low level of intelligence, but they will certainly behave according to the nature of intelligence embedded into them by the software developer. It means they will act as per the wishes of software developer, because they are the ones who have the capacity to control the mind of these devices. Therefore next time when you watch a smart TV (which can be compared to the ‘Telescreen’ of ‘1984’) that has been connected to the Internet and contains some or other form of closed software, then is there any way to tell whether you are watching the TV or the TV is watching at you?

The reason to doubt whether you are watching the TV or the TV is watching you, is mainly because of the closed, proprietary nature of the software written in most of these devices which are heavily guarded by the strong intellectual property rights regime. As a result, no one can inspect or audit the code, and as no one can read the code nobody can understand basically what is written in those programs. All we can do is just depend on the goodwill of the manufacturer of the product and keep on believing that these corporations won't deceive us and that they won't do anything ugly with respect to software. But as we have seen in the case of SONY BMG and Volkswagen, we simply can't trust any corporation, how big and reputed it may be, when it comes to automated programming instructions in the form of closed software. It’s difficult to trust a corporation that writes software behind the closed door.

In the next few years, there is complete possibility that each and every electronic device will get connected to the Internet. Currently we have given a very fancy name to this thing - IoT (Internet of Things). Which is actually a good concept. Once all the devices are connected to the Internet, we can easily control them irrespective of our position or location. We only need to have access to the Internet. It's a very fascinating concept, but the question is who is going to control these devices? ‘You’ or ‘Someone else’ who has access to the Internet and has the knowledge about the software of your device?

Whenever we connect to the Internet via either computer or mobile phone, we keep on believing that we are in complete control of these devices, because they belong to us. But in reality, as soon as we connect to the Internet, we are no longer in real control of our computer or mobile, as now our gadget can be accessed by anyone from anywhere in the world. Then who has the real control? The answer is, it's the people who have written the software or the people who have found a flaw in the given software, that can give them access to the system.

Programmers who have found a flaw in the software and are using it to gain some kind of illegal advantage are known as Crackers.[4] Here one should not get confused with hackers vs crackers. In traditional media, hackers are always conceived in a negative sense as if they are evil in nature and mindset. But actually, ‘hacker’ is a respected terminology in the field of computers and is reserved specifically for expert computer programmers. No programmer can become expert programmer without any experience in hacking. When hackers use their knowledge to do something illegal and damaging, then they are known as Crackers.

Normally whenever something unforeseen happens to the system, we always blame this to Cracker who creates some malware that exploits some loophole in the system. But,we always believe that those who have created a piece of software which is making our system functional and is allowing us to do the work are somewhat sacrosanct, and we should believe them blindly even though their piece of software is closed and heavily guarded, even if we have no idea of what is being written into the code behind the iron curtain. Isn't it contradictory?

Due to this closed nature of software it’s difficult to trust our own computer/mobile or any other device which contains some form of closed software. Because we have no way of knowing whether a piece of software is really doing the work it is supposed to do, or it is doing something more than what is required.

Sometimes in the case of closed software also, it is possible to believe in and trust corporations who are writing it, if there are multiple numbers of corporations competing with each other in free and fair manner in the spirit of competition. But we know that in the real world this is certainly not the case. Most of the electronic hardware and software industries are monopolized by just handful of big corporations. In the case of operating system whether for mobile or desktop segment there are just 2-3 major players in the market who control close to 98 percent of the market share. In the Internet segment more than 50 percent of the Internet ad revenue goes to just one single company. In the case of microchip that powers either the mobile or desktop, there are just 2-3 companies that dominate the entire market. Once a company gets a dominant position in the market or acquire monopoly in a particular sector, it will certainly try to maintain its position. To do this it either takes the help of strong IPR regime or resort to anti-competitive illegal practices. The IPRs which are becoming more and more stringent day-by-day help such companies to strengthen their positions in the market and undermine the entry of any new player in the field. In the last two decades, we have seen that many innovative startups and small firms or companies have been either swallowed by them via acquisition or have been totally destroyed by anti-competitive practices. Anti-competitive practices are even extremely difficult to monitor and catch, in the software industries due to closed nature of software and close alliance between software and hardware vendors. During the ‘First Browser War’[5] in 90’s, Microsoft capitalized its dominance in PC operating system, to win greater share for its own web browser - Internet Explorer, at the expense of its main competitor Netscape

Navigator,[6] and killed one of the most innovative companies of that time. Many times software and hardware vendors collaborate with each other and make adjustment to their systems in such a way that the hardware can't be used by some third party software.[7] As a result, monopolistic tendencies are on the rise especially in the field of computer and Internet. And when such is the case, then we have every reason in the world to doubt the mind that is being inserted into the devices by the corporations.

Basically all the corporations are driven by the motive of profit in this capitalist economy. Hence everyone thinks that these corporations won't deceive their customers, otherwise they will lose their credibility, their customers and hence their share in the market. But when players in the markets are themselves limited in number, customers simply don't have any choice other than accepting what is given to them. Therefore, when they give us closed software and ask us to trust it blindly just on the basis of brand value, then we have every possible reason not to trust them.