Have you ever felt that things are moving really fast? That the dizzying surge of technological advancement is beyond control? That we need to pause a second before we accept a world where vehicles are being driven by themselves, shadowy data firms can swing elections, and AI can determine if a person will become a criminal? You're not the only one. Authors Brad Smith and Carol Ann Browne of Microsoft might concur with you. Not that we have retreated to some kind of pre-technological cave; however, that we have to fix things.

In order to do that, governments and big tech corporations have to work together intelligently. By them collaborating with one another, they can make sure that the digital revolution carries with it the sort of technologies we require immediately: those that enable us to solve our great collective difficulties and make life much simple for a lot of us. If they don't collaborate, then we encounter a very darker timeline – one whereby hackers can shut down hospitals, or hostile-state actors can make use of the internet to hinder our democratic process.

This summary describes Brad Smith and Carol Ann Browne's understandings into present-day technology and provides a window into a future world – which could either be frightening or wonderful, that is reliant on how we behave now.

Data has constantly been an essential aspect of human civilization.

We've regularly depended on data. The entire human civilizations have transferred information from one generation to the other. Without being able to document our methods, it wouldn't have been possible for us to make progress.

In absence of the scrolls of antiquity, our great architectural techniques wouldn't have advanced throughout centuries, mathematical solutions wouldn't have gone from one mind to the other, and military approaches wouldn't have gone from Caesar's battlefields to Napoleon's.

The time when Johannes Gutenberg developed the printing press, there was something of a data explosion. As a lot of people got access to the successes of humankind through the printed word, a democratic revolution started. This had big costs for religion, politics and cultural life.

After, the rise of commerce in the nineteenth and twentieth centuries signified a growing rise in the amount of data in the world. During the mid-twentieth century, there were filing cabinets with abundant data in all organizations, for all possible aim.

Presently, through digitization, we keep a quantity of data unthinkable at any other time in history. This is known as digital architecture the cloud.

Although this word brings to our attention a fluffy, soft cumulus floating overhead us, the reality is similar to a fortress. The cloud has a real physical reality. Each and every time you check for something on your mobile device, you are taking a piece of information from a huge data center.

These are modern wonders that nearly no one gets to experience. Use the one in Quincy – a small town that is nearly 150 miles east of Seattle. In that place, there are two campuses with over 20 huge, nondescript buildings. Each building has the size of a football pitch and can easily contain two large commercial airplanes.

At the core of each building is a computer center, where a lot of servers are arranged in long racks. Somewhere, in one of these buildings, every one of us will possess our own digital file. In one of these buzzing, cavernous rooms, our photographs are there, private emails, and bank account information.

More amazing is the fact that every data center has a precise duplicate, with another set of buildings, similar to the one in Quincy, somewhere else. This manner, if there's a natural or human-made tragedy, our data – our memories, messages, private details – will be stored safely.

Edward Snowden reignited the ancient inquiry of privacy for the twenty-first century.

On the 6th of June 2013, Dominic Carr, the leader of Microsoft's public communications team, got an email whereby the content in the email would surprise him, and then the world.

The email was from a Guardian journalist, who asserted that the US government's National Security Agency (NSA) had been accessing private user information, phone records and other information that belongs to millions of people as well as foreign leaders around the world.

The person that said this story was Edward Snowden, a 29-year-old computer systems administrator that was working at the NSA Threat Operation Centre in Hawaii. He'd downloaded more than 1.5 million confidential documents and then traveled to Hong Kong before telling the Guardian and Washington Post about his story.

What he'd exposed was that the NSA, in association with the British government, had been hacking into undersea fiber-optic cables to duplicate data from Yahoo and Google networks. Microsoft, whose own user info was endangered, was shocked.

At this point, Snowden's disclosures led to a clash between the people and their government that had profound roots. The question of the exact privacy a private citizen need to have has a long history, and Snowden was only the newest person to present it.

John Wilkes was one of the first and he was a British MP of the eighteenth century. He was known for writing crucial speeches on the monarchy and the prime minister of the day.

Eventually, a specific offensive letter made the government grant a warrant for his arrest, enabling them to search any house without warning. The law in Wilkes' day gave small protection from trespass – the king's soldiers could go into any place without sound doubt. Therefore, a lot of doors were broken down, trunks looted and private belongings were taken as proof. They arrested about 49 people in their search for Wilkes, virtually they were all innocent.

Wilkes was eventually arrested; however, decided to fight his case in the courts – and the manner in which he was hunted. To the establishment's surprise, he won.

As part of his case, the courts ruled that authorities need to have a better reason to hold a search. The British press praised the ruling, stating that "all Englishman's house is like his castle and it is not meant to be searched."

In a lot of ways, Wilkes' case led to the start of modern privacy rights. It was an issue reignited by Edward Snowden in 2013 when he exposed again the age-old trend of governments to intrude on their citizens' private lives.

Tech companies were obliged to explain their privacy policies as a result of terrorist attacks.

As the twenty-first century began, terrorist attacks turned out to be a disturbingly repeated incidence.

Initially, the consequences of new digital technologies weren't apparent. For example, 9/11, happened in a world that wasn't yet obsessed with social media, an era of fax machines instead of smartphones.

However, a more recent event, such as the Charlie Hebdo attack in 2015, exposed a new association between technology and terrorism. Brad Smith, Microsoft's president was in his office in Redmond, Seattle, when he first watched the news from Paris. Two brothers, connected with Al-Qaeda, had gone into the headquarters of the satirical magazine Charlie Hebdo and gunned down 12 people. Just like a lot of people in the world, he was extremely troubled by the news. But, he didn't know that the attack would include Microsoft as well.

Very early in the following day, the FBI, in communication with the French authorities, demanded the right to use the terrorists' email account details, in order for them to be tracked. In a period of 45 minutes, Smith's team at Microsoft saw the account information and handed them over to the FBI. The following day, the two attackers were found by the means of various sources and IP addresses and were murdered in a shootout with the police.

An incident just like the Charlie Hebdo attack showed a clear and crucial case for giving security forces the user info they wanted. But, as the Edward Snowden disclosures had revealed, there were a lot of private people and businesses who posed no instant threat; however whose data had been accessed. After every new terror attack, the surveillance state's net became tighter – governments started to ask more data on citizens who were in no way related to terrorism.

In the United States, the government kept requesting for details of people they were inspecting from tech companies. While they were doing this, they set gagging orders, laws that forbade the tech companies from informing their customers about what was going on.

It required nonstop demands from the US government for information for Microsoft to take positive action. Eventually, they decided to sue the government.

In the Supreme Court, the judges concluded that Microsoft had a case against the government, that was, under the First Amendment, they had the right to tell customers that their information was being used. This win made the Department of Justice have a talk with the tech companies and talk about the future. They came to the conclusion that the gagging orders would have boundaries.

This was a vital first step toward good judgment – the stability between accountability and privacy.

Differences in culture and history influence how various nations deal with the question of data privacy.

A lot of the tech innovations of the twenty-first century were created in Silicon Valley in California. That signifies that they were created with a specific cultural perspective in a country that doesn't care about freedom. However, what takes place when this clashes with different views?

One case demonstrates this very well.

In 2018, while the author was in Berlin for different meetings, the authors visited an ancient East German prison and they were taken there by their German Microsoft colleagues. In the prison, they encountered a 75-year-old former prisoner named Hans-Jochen Scheidler, who'd been locked in the miserable, brutalist building for several months for distributing pamphlets condemning the socialist regime. Like a lot of protesters, he'd been captured by the Stasi – the secret police.

That was where the author’s German colleagues noticed an association between the past and present. The Stasi had reserved a huge store of data on East Germans such as Scheidler, gathered by a large network of spies and citizen informers. It was one of the biggest pools of information about a country’s population before the digital era.

The German colleagues identified that this was the reason why Germany was really careful than the United States about huge data collection. That was the reason why, as a country, they thought of ethical questions before mere commercial interests.

This gave an extreme impression on Microsoft’s president. It discovered how international data storage would have international difficulties. And it signified that Microsoft would carry out a cautious analysis of their data policies. They would need to evaluate where they selected to permit data storage centers to be made.

For example, nations with troubling human rights records would not be permitted to have any access to their citizens’ data, while those with slight autocratic, however still doubtful records, would be allowed to store secondary data – that connecting to businesses, for example.

The perfect surroundings for big tech companies are nations with stable political conditions and strong human rights legislation. For several years, this has been the Republic of Ireland, which, with its place in the EU, accepting migration policy and tax incentives, has been a huge draw for big tech back in the 1980s.

But, as we understand, the route to totalitarianism can be brief, thus present stability is no warranty for the future. These are questions with which the world will deal with in decades to come. We need to hope, that during that time, tech companies are fixed.

The world presently hasn’t woken up to the whole consequences of cyberwar.

On the 12th of 2017, the owner of an ice cream business, Patrick Ward was taken into a surgical prep room at St Bartholomew's hospital in central London. He’d traveled three hours from a small village in southern England to the hospital for the critical heart surgery that he'd waited for two years to do. He was on a gurney, wired up to monitors, with his chest shaved. A surgeon's assistant came and said to him that he'd only have a few more minutes to wait.

He waited, hours after hours passed. Then, a doctor opened the doors of the prep room and told him that he wouldn't undergo his surgery because all the hospital's computers were down.

From thousands of miles away, hackers had initiated a cyberattack that had made the entire system useless and weaken a third of the National Health Service.

The cyberattack destroyed the United Kingdom and Spain before dispersing to the remaining part of the world, affecting close to three hundred thousand computers in over 150 countries. The malware locked Windows operating systems and requested a payment of $300 for a password that could unfreeze the computer again. Aptly, the attack was called "WannaCry" after it brought many computer users to tears.

Afterward, it became known that the malware used was created by the United States government; however was stolen from them and leaked on the dark web, maybe to a mean state actor. As a matter of fact, it was highly assumed that North Korea had created that attack in vengeance against a previous one by the United States.

The fact that the malware was really easy to steal shocked tech corporations such as Microsoft, who mentioned that it was as if the American government had been so careless to just leave a pile of Tomahawk missiles lying all over the place.

That wasn't an exaggeration. Although the malware was immediately fixed, and people such as Patrick Ward were able to have their works, the likely repercussions of more extreme cyberattacks were disturbing.

Think of a future where the malware is really difficult to decode – where automatic vehicles could be hacked from far away distance and sent spiraling out of control, where banks could be closed down, where patients' life support system could be turned off. If we're not careful, this is the type of future we'll have soon.

Social media platforms have been used to disseminate conflict in present democracies in a manner that emulates history.

In its early stages, the internet looked like a good means to connect the world and bring us closer to one another; however, recently we've realized its dark aspect.

Consider the disruptive 2016 US election, where social media platforms were used to spread "fake news."

Operating from St Petersburg, Russian operatives from the Internet Research Agency (IRA) made deceptive stories about Hillary Clinton, displayed on absolutely fake websites. These went viral across the internet, "seeded" by a few nodes, certain websites that would reach various kinds of internet users. These stories were basically about Clinton's alleged ill health, her supposed association to pedophile networks, and other alike shocking lies.

On social media platforms, these stories worked their way around specific online communities while other communities were unaware of the stories. This is how online issues are made, with people becoming more and more polarized, sometimes trusting things that are not even true at all.

One of the most severe repercussions of this kind of manipulation was in 2016 with the IRA's successful effort to form an anti-Trump protest and a pro-Trump counter-protest in Houston, Texas. American yelled at American, both ignorantly annoyed and sent into a rage by a person sitting at a computer in St Petersburg.

Even though this might seem like a new threat, foreign actors have continuously had the power to make the conflict in other countries. For example, in 1793, when Britain and France went to war, a French ambassador known Edmond Charles Genêt got to America only a few weeks after President George Washington had confirmed his nation's neutrality. Genêt was on a task to make the young republic support France and initiated tensions in Washington's cabinet straight away.

After a short time, the French ambassador appealed to the American public one on one for their support, strengthening a bitter separation in the population. Quite abruptly, the political debate turned out to be intense, street fights occurred and friendships were damaged.

Eventually, Washington’s divided cabinet reasoned together with one aim: to send Genêt back to France before he could create more problems. Regardless of their dispute on the Franco-British war, they decided that no outside effect could be permitted to cause such separation again. This occurrence stirred Washington to say in his farewell speech that “A free people should be regularly awake because history and experience attest that foreign influence is one of the greatest destructive enemies of republican government.”

Considering Kremlin's effort to obstruct the 2016 US election, these words hold a contemporary weight.

AI has brought up some difficult issues.

Artificial Intelligence: what comes to your mind first? The dark techno score and scanner gaze of The Terminator? R2D2? The AI romance in the film Her? The reality is, we’re surrounded by AI already: for example, your smartphone studies things about you as you make use of them.

Therefore, what should matter to us about AI today?

There is a general terror that developing AI will lead to all-powerful machine overlords. Presently that AI is linked to the cloud – the biggest store of data that has ever occurred– there is a concern that machine learning will accelerate to such a level that a superintelligence will occur. The amalgamation of this entire data would be known as Singularity, and it would breed increasingly sophisticated AI.

But, up to now, this is a science fiction fantasy. There are genuine worries with AI in the here and now, and they say a lot about the human beings that made the computers than the technology itself.

The main worry, in fact, is the bias that is in AI. For example, during a tech conference at the White House in 2016, all the focused changed to an article in the magazine called ProPublica titled “Machine Bias.” The article’s subtitle described the worry: “There’s software used around the country to guess future criminals. And it’s biased against blacks.”

This bias occurred because of the issue of unreliable data sets. For example, let’s look at facial recognition technology. A facial recognition data set might contain enough photos of white males to forecast, with a high precision rate, the faces of white men. However, if there are lesser data of women or people of color, then more mistakes with these demographics are possible.

A related conclusion to the ProPublica article was discovered in research by Joy Buolamwini the poet and scholar and Timnit Gebru, a Stanford University researcher. During their research on facial recognition technology, they discovered bad accuracy rates for black politicians in Africa compared to white politicians in Europe.

Significantly, their work uncovered another aspect of bias. This involved the teams that created new technologies. They discovered that, except tech teams considered the diversity of the world, it was really possible that their inventions would have prejudicial blind spots.

Also, they discovered that a more diverse group of researchers and engineers was very likely to notice complications in the design since bias was something that impacted them personally.

New technologies can be utilized positively; however, combined thinking is needed.

A device can be utilized for either good or evil. You can either sweep a kitchen floor or smash someone’s head with a broom. The same goes for information technology.

Look at these recent innovations:

At Princeton College, a professor named Marina Rustow of Near Eastern studies is trying to decode a trove of four hundred thousand documents from Cairo’s Ben Ezra Synagogue. It’s the biggest recorded cache of Jewish manuscripts in the whole world. Certainly, learning these documents is a difficult challenge –a lot of them are in pieces or dispersed in archives around the world. This cause physically combining them together unachievable

But, using advanced AI, Rustow's team was able to combine digital fragments that are thousands of miles away with speed and accuracy that nobody could achieve. This has signified that Rustow has been able to know a formerly little-known aspect of the Middle Ages, whereby Jews and Muslims lived peacefully.

Likewise, AI can be used to keep the living world. Microsoft's AI for Earth team has created a program that assists park rangers in Uganda defend against poachers. By making use of an algorithm, the rangers can detect poaching activity, which enables them to proactively recognize poaching places.

These are only two methods in which technology can be used for an advantage purpose. But, if we're to make this the aim moving forward, large-tech and governments must work together more.

First of all, tech companies can consider themselves as unaccountable to the world anymore. There has to be a wider deliberation of aims, outside only commercial interests. Instead of just contending with other firms, the leaders of big tech – as people who exert huge power –require combined thinking around their moral responsibilities.

Secondly, governments need to know and regulate technology if this world is to turn into reality. Government officials are responsible to educate themselves on developing tech. it is no longer allowed for officials to be unaware of something really transformative –just like the US senator the authors mention, who didn't know that he could read the Washington Post online. In terms of regulation – no one would see it appropriate for the aviation industry to be unregulated; hence why should something that is really dangerous as digital technology goes unchecked?

Thus, this is the plan for the future – a world where we learn about technology for positive effects, or one where it masters us. We have to decide– fast.

Tools and Weapons: The Promise and the Peril of the Digital Age by Brad Smith, Carol Ann Browne Book Review

New digital technologies offer us amazing opportunities, however; with also unpredicted threats. We can either learn these inventions for good, like making use of AI to combat poaching and climate change, or we can let their darker potential to be controlled by hostile actors. In order to make sure that technology is a drive for good, it is important that tech companies work with governments on regulation and an ethical structure.

When you read a news story, ensure it can be confirmed.

When you browsing on the internet and you see some certain provocative headline, see that it's based on the truth. This is what you can do. Check if a lot of highly-viewed sources repeat the exact story. If they don't, and it's restricted to just a source, be vigilant that you're not being deceived!

https://goodbooksummary.com/tools-and-weapons-by-brad-smith-carol-ann-browne-book-summary/