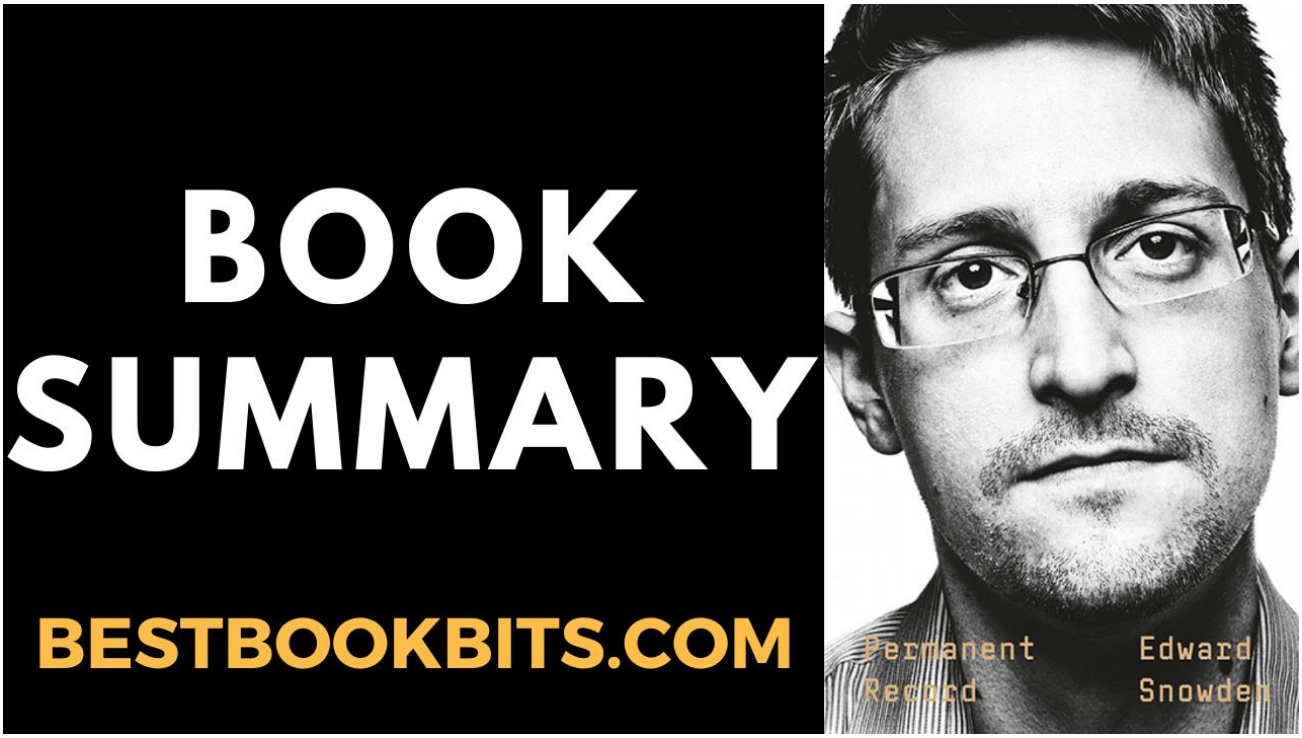

- My name is Edward Joseph Snowden. I used to work for the government, but now I work for the public.

- I used to be—a spy for the Central Intelligence Agency (CIA) and National Security Agency (NSA), just another young technologist out to build what I was sure would be a better world.

- My career in the American Intelligence Community (IC) only lasted a short seven years,

- I participated in the most significant change in the history of American espionage—the change from the targeted surveillance of individuals to the mass surveillance of entire populations. I helped make it technologically feasible for a single government to collect all the world's digital communications, store them for ages, and search through them at will.

- The doors to the most secretive intelligence agencies were flung wide open to young technologies like myself. And so the geek inherited the earth.

- At twenty-two, I got my first top secret clearance from the NSA, for a position at the very bottom of the org chart. Less than a year later, I was at the CIA, as a systems engineer with sprawling access to some of the most sensitive networks on the planet.

- From 2007 to 2009, I was stationed at the US Embassy in Geneva as one of the rare technologists deployed under diplomatic cover, tasked with bringing the CIA into the future by bringing its European stations online, digitizing and automating the network by which the US government spied.

- My generation did more than reengineer the work of intelligence; we entirely redefined what intelligence was. For us, it was not about clandestine meetings or dead drops, but about data.

- By age twenty-six, I was a nominal employee of Dell, but once again working for the NSA. Contracting had become my cover, as it was for nearly all the tech-inclined spies of my cohort.

- I was sent to Japan, where I helped to design what amounted to the agency's global backup—a massive covert network that ensured that even if the NSA's headquarters was reduced to ash in a nuclear blast, no data would ever be lost. At the time, I didn't realize that engineering a system that would keep a permanent record of everyone's life was a tragic mistake.

- I came back to the States at age twenty-eight, and received a stratospheric promotion to the technical liaison team handling Dell's relationship with the CIA. My job was to sit down with the heads of the technical divisions of the CIA in order to design and sell the solution to any problem that they could imagine. My team helped the agency build a new type of computing architecture—a "cloud," the first technology that enabled every agent, no matter where they were physically located, to access and search any data they needed, no matter the distance.

- In sum, a job managing and connecting the flow of intelligence gave way to a job figuring out how to store it forever, which in turn gave way to a job making sure it was universally available and searchable. These projects came into focus for me in Hawaii, where I moved to take a new contract with the NSA at the age of twenty-nine. Up until then, I'd been laboring under the doctrine of Need to Know, unable to understand the cumulative purpose behind my specialized, compartmentalized tasks. It was only in paradise that I was finally in a position to see how all my work fit together, meshing like the gears of a giant machine to form a system of global mass surveillance.

- Deep in a tunnel under a pineapple field—a subterranean Pearl Harbor-era former airplane factory –I sat at a terminal from which I had practically unlimited access to the communications of nearly every man, woman, and child on earth who'd ever dialed a phone or touched a computer. Among those people were about 320 million of my fellow American citizens, who in the regular conduct of their everyday lives were being surveilled in gross contravention of not just the Constitution of the United States, but the basic values of any free society.

- I did a dangerous thing for a man in my position: I decided to tell the truth. I collected internal IC documents that gave evidence of the US government's lawbreaking and turned them over to journalists, who vetted and published them to a scandalized world.

- the beginning of surveillance capitalism, and the end of the Internet

- That new product was Us.

- Our attention, our activities, our locations, our desires—everything about us that we revealed, knowingly or not, was being surveilled and sold in secret,

- The American government, in total disregard of its founding charter, fell victim to precisely this temptation, and once it had tasted the fruit of this poisonous tree it became gripped by an unrelenting fever. In secret, it assumed the power of mass surveillance, an authority that by definition afflicts the innocent far more than the guilty.

- The system of near-universal surveillance had been set up not just without our consent, but in a way that deliberately hid every aspect of its programs from our knowledge.

- The freedom of a country can only be measured by its respect for the rights of its citizens,

- It's been six years since I came forward because I witnessed a decline in the commitment of so-called advanced governments throughout the world to protecting this privacy, which I regard and the United Nations regards—as a fundamental human right.

- In the span of those years, however, this decline has only continued as democracies regress into authoritarian populism. Nowhere has this regression been more apparent than in the relationship of governments to the press.

- The attempts by elected officials to delegitimize journalism have been aided and abetted by a full-on assault on the principle of truth. What is real is being purposefully conflated with what is fake, through technologies that are capable of scaling that conflation into unprecedented global confusion.

- I know this process intimately enough, because the creation of irreality has always been the Intelligence Community's darkest art. The same agencies that, over the span of my career alone, had manipulated intelligence to create a pretext for war—and used illegal policies and a shadow judiciary to permit kidnapping as "extraordinary rendition," torture as "enhanced interrogation," and mass surveillance as "bulk collection"—didn't hesitate for a moment to call me a Chinese double agent, a Russian triple agent, and worse: "a millennial."

- Life only scrolls in one direction, which is the direction of time, and no matter how far we might manage to go, that invisible wall will always be just behind us, cutting as off from the past, compelling us on into the unknown.

- As the millennium approached, the online world would become increasingly centralized and consolidated, with both governments and businesses accelerating their attempts to intervene in what had always been a fundamentally peer-to-peer relationship. But for one brief and beautiful stretch of time—a stretch that, fortunately for me, coincided almost exactly with my adolescence—the Internet was mostly made of, by, and for the people. Its purpose was to enlighten, not to monetize, and it was administered more by a provisional cluster of perpetually shifting collective norms than by exploitative, globally enforceable terms of service agreements. To this day, I consider the 1990s online to have been the most pleasant and successful anarchy I've ever experienced.

- In the 1990s, the Internet had yet to fall victim to the greatest iniquity in digital history: the move by both government and business to link, so intimately as possible, users' online personas to their offline legal identity.

- In the new millennium, Internet technology would be turned to very different ends: enforcing fidelity to memory, identarian consistency, and so ideological conformity.

- To grow up is to realize the extent to which your existence has been governed by systems of rules, vague guidelines, and increasingly unsupportable norms that have been imposed on you without your consent and are subject to change at a moment's notice.

- I realized that any opposition to this system would be difficult, not least because getting its rules changed to serve the interests of the majority would involve persuading the rule makers to put themselves at a purposeful disadvantage. That, ultimately, is the critical flaw or design defect intentionally integrated into every system, in both politics and computing: the people who create the rules have no incentive to act against themselves.

- What convinced me that school, at least, was an illegitimate system was that it wouldn't recognize any legitimate dissent.

- However, the benevolent tyranny of school, like all tyrannies, has a limited shelf life. At a certain point, the denial of agency becomes a license to resist.

- though it's characteristic of adolescence to confuse resistance with escapism or even violence.

- This is the origin of all hacking: the awareness of a systematic linkage between input and output, between cause and effect. Because hacking isn't just native to computing—it exists wherever rules do. To hack a system requires getting to know its rules better than the people who created it or are running it, and exploiting all the vulnerable distance between how those people had intended the system to work and how it actually works, or could be made to work. In capitalizing on these unintentional uses, hackers aren't breaking the rules as much as debunking them.

- Humans are hardwired to recognize patterns. All the choices we make are informed by a cache of assumptions, both empirical and logical, unconsciously derived and consciously developed. We use these assumptions to assess the potential consequences of each choice, and we describe the ability to do all of this, quickly and accurately, as intelligence. But even the smartest among us rely on assumptions that we've never put to the test—and because we do, the choices we make are often flawed. Anyone who knows better, or thinks more quickly and more accurately than we do, can take advantage of those flaws to create consequences that we never expected. It's this egalitarian nature of hacking ---which doesn't care who you are, just how you reason—that makes it such a reliable method of dealing with the type of authority figures so convinced of their system's righteousness that it never occurred to them to test it.

- You should always let people underestimate you. Because when people misappraise your intelligence and abilities, they're merely pointing out their own vulnerabilities—the gaping holes in their judgment that need to stay open if you want to cartwheel through later on a flaming horse, correcting the record with your sword of justice.

- The Intelligence Community tries to inculcate in its workers a baseline anonymity, a sort of blank-page personality upon which to inscribe secrecy and the art of imposture. You train yourself to be inconspicuous, to look and sound like others. You live in the most ordinary house, you drive the most ordinary car, you wear the same ordinary clothes as everyone else. The difference is, you do it on purpose: normalcy, the ordinary, is your cover. This is the perverse reward of a self-denying career that brings no public glory: the private glory comes not during work, but after, when you can go back out among other people again and successfully convince them that you're one of them.

- Though there are a score of more popular and surely more accurate psychological terms for this type of identity split, I tend to think of it as human encryption. As in any process of encryption, the original material—your core identity—still exists, but only in a locked and scrambled form. The equation that enables this ciphering is a simple proportion: the more you know about others, the less you know about yourself. After a time, you might forget your likes and even your dislikes. You can lose your politics, along with any and all respect for the political process that you might have had. Everything gets subsumed by the job, which begins with a denial of character and ends with a denial of conscience. "Mission First."

- an autobiographical statement is static, the fixed document of a person in flux. This is why the best account that someone can ever give of themselves is not a statement but a pledge—a pledge to the principles they value, and to the vision of the person they hope to become.

- We can't erase the things that shame us, or the ways we've shamed ourselves, online. All we can do is control our reactions—whether we let the past oppress us, or accept its lessons, grow, and move on.

- I'm going to press Pause here, for a moment, to explain something about my politics at age twenty-two: I didn't have any. Instead, like most young people, I had solid convictions that I refused to accept weren't truly mine but rather a contradictory cluster of inherited principles. My mind was a mash-up of the values I was raised with and the ideals I encountered online. It took me until my late twenties to finally understand that so much of what I believed, or of what I thought I believed, was just youthful imprinting. We learn to speak by imitating the speech of the adults around us, and in the process of that learning we wind up also imitating their opinions, until we've deluded ourselves into thinking that the words we're using are our own.

- the work of American Intelligence is done as frequently by private employees as it is by government servants.

- THE AGENCIES WERE hiring tech companies to hire kids, and then they were giving them the keys to the kingdom, because –as Congress and the press were told—the agencies didn't have a choice. No one else knew how the keys, or the kingdom, worked.

- the great nexus of the Intelligence Community and the tech industry: both are entrenched and unelected powers that pride themselves on maintaining absolute secrecy about their developments. Both believe that they have the solutions for everything, which they never hesitate to unilaterally impose. Above all, they both believe that these solutions are inherently apolitical, because they're based on data, whose prerogatives are regarded as preferable to the chaotic whims of the common citizen.

- Being indoctrinated into the IC, like becoming expert at technology, has powerful psychological effects. All of a sudden you have access to the story behind the story, the hidden histories of well-known, or supposedly well-known, events. That can be toxicating, at least for a teetotaler like me. Also, all of a sudden you have not just the license but the obligation to lie, conceal, dissemble, and dissimulate. This creates a sense of tribalism, which can lead many to believe that their primary allegiance is to the institution and not to the rule of law.

- it’s not like there’s a lot to be found out there on the public Internet that’s more interesting than what the agency already has internally. Few realize this, but the CIA has its own Internet and Web. It has its own kind of Facebook, which allows agents to interact socially; its own type of Wikipedia, which provides agents with information about agency teams, projects, and missions; and its own internal version of Google—actually provided by Google—which allows agents to search this sprawling classified network. Every CIA component has its own website on this network that discuss what it does and posts meeting minutes and presentations.

- The Tor Project was a creation of the state that ended up becoming one of the few effective shields against the state’s surveillance. Tor is free and open-source software that, if used carefully, allows its users to browse online with the closest thing to perfect anonymity that can be practically achieved at scale. Its protocols were developed by the US Naval Research Laboratory throughout the mid-1990s, and in 2003 it was released to the public—to the worldwide civilian population on whom its functionality depends. This is because Tor operates on a cooperative community model, relying on tech-savvy volunteers all over the globe who run their own Tor servers out of their basements, attics, and garages. By routing its users’ Internet traffic through these servers, Tor does the same job of protecting the origin of that traffic as the CIA’s “non-attributable research” system, with the primary difference being that Tor does it better, or at least more efficiently. I was al

- Sitting around discussing how to hack a faceless UN complex was psychologically easier by a wide margin. Direct engagement, which can be harsh and emotionally draining, simply doesn’t happen that much on the technical side of intelligence, and almost never in computing. There is a depersonalization of experience fostered by the distance of a screen. Peering at life through a window can ultimately abstract us from our actions and limit any meaningful confrontation with their consequences.

- The Internet is fundamentally American, but I had to leave America to fully understand what that meant. The World Wide Web might have been invented in Geneva, at the CERN research laboratory in 1989, but the ways by which the Web is accessed are as American as baseball, which gives the American Intelligence Community the home field advantage. The cables and satellites, the servers and towers—so much of the infrastructure of the Internet is under US control that over 90 percent of the world’s Internet traffic passes through technologies developed, owned, and/or operated by the American government and American businesses, most of which are physically located on American territory.

- The NSA’s conventional wisdom was that there was no point in collecting anything unless they could store it until it was useful, and there was no way to predict when exactly that would be. This rationalization was fuel

- for the agency's ultimate dream, which is permanency—to store all of the files it has ever collected or produced for perpetuity, and so create a perfect memory. The permanent record.

- the fundamental rule of technological progress: if something can be done, it probably will be done, and possibly already has been. There was simply no way for America to have so much information about what the Chinese were doing without having done some of the very same things itself, and I had the sneaking sense while I was looking through all this China material that I was looking at a mirror and seeing a reflection of America. What China was doing publicly to its own citizens, America might be—could be—doing secretly to the world.

- STELLARWIND was the classified report's deepest secret. It was, in fact, the NSA's deepest secret, and the one that the report's sensitive status had been designed to protect. The program's very existence was an indication that the agency's mission had been transformed, from using technology to defend America to using technology to control it by redefining citizens' private Internet communications as potential signals intelligence.

- A single current-model smart phone commands more computing power than all of the wartime machinery of the Reich and the Soviet Union combined. Recalling this is the surest way to contextualize not just the modern American IC's technological dominance, but also the threat it poses to democratic governance.

- Digital technology didn't just further streamline such accounting—it is rendering it obsolete. Mass surveillance is now a never-ending census, substantially more dangerous than any questionnaire sent through the mail. All our devices, from our phones to our computers, are basically miniature census—takers we carry in our backpacks and in our pockets—census-takers that remember everything and forgive nothing.

- The generations to come would have to get used to a world in which surveillance wasn't something occasional and directed in legally justified circumstances, but a constant and indiscriminate presence: the ear that always hears, the eye that always sees, a memory that is sleepless and permanent.

- Once the ubiquity of collection was combined with the permanency of storage, all any government had to do was select a person or a group to scapegoat and go searching.

- The data we generate just by living—or just by letting ourselves be surveilled while living—would enrich private enterprise and impoverish our private existence in equal measure. If government surveillance was having the effect of turning the citizen into a subject, at the mercy of state power, then corporate surveillance was turning the consumer into a product, which corporations sold to other corporations, data brokers, and advertisers.

- Read your terms of service agreements for cloud storage, which get longer and longer by the year—current ones are over six thousand words, twice the average length of one of these book chapters. When we choose to store our data online, we're often ceding our claim to it. Companies can decide what type of data they will hold for us, and can willfully delete any data they object to. Unless we've kept a separate copy on our own machines or drives, this data will be lost to us forever. If any of our data is found to be particularly objectionable or otherwise in violation of the terms of service, the companies can unilaterally delete our accounts, deny us our own data, and yet retain a copy for their own records, which they can turn over to the authorities without

our knowledge or consent. Ultimately, the privacy of our data depends on the ownership of our data. There is no property less protected, and yet no property more private.

- The politics of terror became more powerful than the terror itself, resulting in "counterterror": the panicked actions of a country unmatched in capability, unrestrained by policy, and blatantly unconcerned about upholding the rule of law. After 9/11, the IC's orders had been "never again," a mission that could never be accomplished. A decade later, it had become clear, to me at least, that the repeated evocations of terror by the political class were not a response to any specific threat or concern but a cynical attempt to turn terror into a permanent danger that required permanent vigilance enforced by unquestionable authority. After a decade of mass surveillance, the technology had proved itself to be a potent weapon less against terror and more against liberty itself. By continuing these programs, by continuing these lies, America was protecting little, winning nothing, and losing much—until there would be few distinctions left between those post – 9/11 polarities of "Us" and "Them."

- in a truly just society the people were not answerable to the government, the government was answerable to the people.

- and its own specific goals, they all had one thing in common: a rejection of authoritarianism, a recommitment to the humanitarian principle that an individual's rights are inborn and inalienable.

- In an authoritarian state, rights derive from the state and are granted to the people. In a free state, rights derive from the people and are granted to the state.

- It's this clash, between the authoritarian and the liberal democratic, that I believe to be the major ideological conflict of my time—not some concocted, prejudiced notion of an East-West divide, or of a resurrected crusade against Christendom or Islam.

- Authoritarian states are typically not governments of laws, but governments of leaders, who demand loyalty from their subjects and are hostile to dissent. Liberal—democratic states, by contrast, make no or few such demands, but depend almost solely on each citizen voluntarily assuming the responsibility of protecting the freedoms of everyone else around them, regardless of their race, ethnicity, creed, ability, sexuality, or gender.

- Americans only have a "right" to free speech because the government is forbidden from making any law restricting that freedom, and a "right" to a free press because the government is forbidden from making any law to abridge it. They only have a "right" to worship freely because the government is forbidden from making any law respecting an establishment of religion, and a "right" to peaceably assemble and protest because the government is forbidden making any law that says they can't.

- Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say. Or that you don't care about freedom of the press because you don't like to read. Or that you don't care about freedom of religion because you don't believe in God.

- The most important decisions in life are never made that way. They're made subconsciously and only express themselves consciously once fully formed—once you're finally strong enough to admit to yourself that this is what your conscience has already chosen for you, this is the course that your beliefs have decreed.

- in mid – 2012, I was just trying to get a handle on how mass surveillance actually worked. Almost every journalist who later reported on the disclosures was primarily concerned with the targets of surveillance –the efforts to spy on American citizens, for instance, or on the leaders of America's allies. That is to say, they were more interested in the topics of the surveillance reports than in the system that produced them.

- NSA's new surveillance posture as a matter of six protocols: "Sniff It All, Know It All, Collect It All, Process It All, Exploit It All, Partner It All." This was just PR speak, marketing jargon. It was intended to impress America's allies: Australia, Canada, New Zealand, and the UK, the primary countries with which the United States shares intelligence. (Together with the United States, these countries are known as the Five Eyes.)

- finding out what that data was; "Collect It All" meant capturing that data; "Process It All" meant analyzing that data for usable intelligence; "Exploit It All" meant using that intelligence to further the agency's aims; and "Partner It All" meant sharing the new data source with allies.

- our clouds, computers, and phones have become our homes, just as personal and intimate as our actual houses nowadays. If you don't agree,

- then answer me this: Would you rather let your coworkers hang out at your home alone for an hour, or let them spend even just ten minutes alone with your unlocked phone?

- The constitutional system only functions as a whole if and when each of its three branches works as intended. When all three don't just fail, but fail deliberately and with coordination, the result is a culture of impunity. I realized that I was crazy to have imagined

- that the Supreme Court, or Congress, or President Obama, seeking to distance his administration from President George W. Bush's would ever hold the IC legally responsible—for anything. It was time to face the fact that the IC believed themselves above the law, and given how broken the process was, they were right. The IC had come to understand the rules of our systems better than the people who had created it, and they used that knowledge to their advantage. They'd hacked the Constitution.

- AMERICA WAS BORN from an act of treason. The Declaration of Independence was an outrageous violation of the laws of England and yet the fullest expression of what the Founders called the "Laws of Nature," among which was the right to defy the powers of the day and rebel on point of principle, according to the dictates of one's conscience. The first Americans to exercise this right, the first "whistleblowers" in American history, appeared one year later—in 1777.

- A "whistleblower," in my definition, is a person who through hard experience has concluded that their life inside an institution has become incompatible with the principles developed in-and the loyalty owed to—the greater society outside it, to which that institution should be accountable. This person knows that they can't remain inside the institution, and knows that the institution can't or won't dismantled. Reforming the institution might be possible, however, so they blow the whistle and disclose the information to bring public pressure to bear.

- I was resolved to bring to light a single, all-encompassing fact: that my government had developed and deployed a global system of mass surveillance without the knowledge or consent of its citizenry.

- "Technology is moving faster than government or law can keep up. It's moving faster….than you can keep up: you should be asking the question of what are your rights and who owns your data."

- In just the seven short years of my career, I'd climbed from maintaining local servers to crafting and implementing globally deployed systems—from graveyard-shift security guard to key master of the puzzle palace.

- XKEYSCORE, which is perhaps best understood as a search engine that lets an analyst search through all the records of your life. Imagine a kind of Google that instead of showing pages from the public Internet returns results from your private email, your private chats, your private files, everything.

- By creating a world-spanning system that tracked these identifiers

- across every available channel of electronic communications, the American Intelligence Community gave itself the power to record and store for perpetuity the data of your life. And that was only the beginning. Because once America's spy agencies had proven to themselves that it was possible to passively collect all of your communications, they started actively tampering with them, too. By poisoning the messages that were headed your way with snippets of attack code, or "exploits," they developed the ability to gain possession of more than just your words. Now they were capable of winning total control of your whole device, including its camera and microphone.

- This is the result of two decades of unchecked innovation—the final product of a political and professional class that dreams itself your master. No matter the place, no matter the time, and no matter what you do, your life has now become an open book.

- law is country-specific, whereas technology is not. Every nation has its own legal code but the same computer code.

- Nearly every country in the world found itself in a similar bind: its citizens outraged, its government complicit. Any elected government that relies on surveillance to maintain control of a citizenry that regards surveillance as anathema to democracy has effectively ceased to be a democracy. Such cognitive dissonance on a geopolitical scale has helped to bring individual privacy concerns back into the international dialogue within the context of human rights. For the first time since the end of World War II, liberal democratic governments throughout the world were discussing privacy as the natural, inborn right of every man, woman, and child. In doing so they were harking back to the 1948 UN Universal Declaration of Human Rights, whose Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Like all UN declarations, this aspirational document was never enforceable, but it had been intended to inculcate a new basis for transnational civil liberties in a world that had just survived nuclear atrocities and attempted genocides and was facing an unprecedented surfeit of refugees and the stateless.

- We are the first people in the history of the planet for whom this is true, the first people to be burdened with data immortality, the fact that our collected records might have an eternal

existence. This is why we have a special duty. We must ensure that these records of our pasts can’t be turned against us, or turned against our children.

- ABOUT THE AUTHOR – EDWARD SNOWDEN was born in Elizabeth City, North Carolina, and grew up in the shadow of Fort Meade. A systems engineer by training, he served as an officer of the Central Intelligence Agency, and worked as a contractor for the National Security Agency. He has received numerous awards for his public service, including the Right Livelihood Award, the German Whistleblower Prize, the Ridenhour Prize for Truth-Telling, and the Carl von Ossietzky Medal from the International League of Human Rights. Currently, he serves as president of the board of directors of the Freedom of the Press Foundation.