# *Rule By Punch Cards*
# *or: How Computers Are A Menace to Liberty*

By Hans Sherrer [1]

*"the right to be let alone - [is] the most comprehensive*
*of rights and the right most valued by civilized men."*
Justice Louis D. Brandeis dissenting in *Olmstead v. U.S. (1928)*

Computers are the greatest menace to human liberty yet created by man. Conceived as a device for the federal government to efficiently compile, analyze and store data about Americans, the very nature of the computer is to impair a person's liberty by undermining their "right to be let alone." As Justice Brandeis lucidly stated in 1928, liberty is directly related to being "let alone." [2] The more the government knows about a person the easier it is for it to interfere with their life by controlling, regulating and taxing them.

The menace of computers to liberty is traceable to its conception and development by a U.S. Census Bureau employee who patented the world's first electro-mechanical computer in 1884. Specifically designed to efficiently compile and analyze information about Americans, that computer's resounding success at processing the 1890 federal census created a demand for its use by governments around the world. In the intervening 100+ years governments have relied on computers to compile detailed dossiers on many hundreds of millions of people. The computer has proven to be such a versatile device that governments have expanded their uses to include such diverse tasks as administering the economy, monitoring the distribution of social services and waging war more efficiently.

Reflecting the computer's origin as a child of the government's desire to count, sort, catalog and keep tabs on Americans, the federal government has been a driving force behind its development up to the present. The government's nurturing of the computer has resulted in its evolvement into a near perfect instrument for interfering with a person's "right to be let alone," and hence undermining their liberty.

## The Menace of the Electro-Mechanical Computer

Governments have long hungered to accumulate information about people living within their geographical confines. That desire is even embodied in the census provision of the U.S. Constitution. [3] Until the 19th Century, however, the gathering of information by governments was limited, slow, and once compiled it was largely inaccessible. Those physical limitations on the government’s ability to invade the privacy of people served as an effective check on its ability to limit their liberty.

The critical event that led to obliteration of technological limitations on the government's invasion of privacy occurred in 1879. During dinner with nineteen year-old Census Bureau worker Herman Hollerith, the federal government's Director of Vital Statistics planted a subconscious seed in Hollerith’s mind when he made the comment: “There ought to be a machine for doing the purely mechanical work of tabulating population and similar statistics.” [4]

A year later Hollerith had a brilliant insight triggered by seeing a train conductor punching tickets in a manner that recorded specific physical characteristics of a passenger. Hollerith’s vision was that a card could be punched with standardized holes representing information, such as an individual's occupational, personal and ethnic characteristics. Hollerith figured the holes in the card would create a *punched photograph* of a person's life readable by a spring mechanism using electrical brush contacts to sense the holes. As the cards were processed, they could be sorted into stacks based on data-specific holes. [5]

Hollerith’s groundbreaking idea was to transform punch cards from their then static uses of merely instructing cloth machines to weave a particular pattern or a piano to play a particular tune, into a dynamic means of recording data about an individual person that could be used to identify and differentiate information about that person from information about any and every other person. Hollerith’s idea for a mechanical brain was much more expansive in its concept and possible applications than the few working mechanical devices that had been invented prior to 1879 to perform mathematical calculations. [6]

Several thousand dollars borrowed from a German friend enabled Herman Hollerith to patent and manufacture a working prototype of his idea by 1884. Its initial test, which it passed with flying colors, was a count of the dead for the local health departments in Maryland, New York, and New Jersey. The electro-mechanical punch card computer proved successful at keeping track of details and analyzing data hundreds of times faster than was possible by hand. However, his device was considered somewhat of a novelty and he didn't produce any for sale. That changed when Hollerith won a contest sponsored by the U.S. Census Bureau for the best device to automate the 1890 Census. [7] The resulting government contract enabled him to manufacture his first machines.

Hollerith's electro-mechanical computer had an immediate impact on the ability of the federal government to collect information about the American population. In 1890, census takers were able to ask 235 *specific* questions: *4,700%* more than in 1870 when they only asked 5 *general* questions. Hollerith's device made it possible for federal officials to view the countries population on punch cards, and to isolate a particular racial, ethnic or religious group. After his success with the 1890 census, Hollerith was hired by Czar Nicholas II in 1895 to provide the same technology for Russia to conduct its first census. [8]

Hollerith's success with the U.S. and Russian census' proved his revolutionary tabulating device was the key governments around the world had been waiting for to unlock Pandora's Box of accumulating a practically unlimited amount of useful information about people under their control. That capability soon attracted government statisticians in many other countries, including England, France, Austria, and Germany. [9]

It was apropos that Hollerith named his company the Tabulating Machine Company (TMC) when he incorporated it in 1896. [10] It is noted in *Psychological Principles in System Development* that Hollerith's innovations - of using punch cards as a memory device to store information for future use and to instruct a computer how data will be processed - were the most important developments in the computer's history. Today's most sophisticated electronic computers continue to use variations of Hollerith's storage and programming ideas. [11]

In 1911, Hollerith sold out to industrialist Charles Flint who combined TMC with his other business enterprises. The evolution of Hollerith's original punch card computer into a sophisticated data-manipulation device was reflected in the new company's name: Computing-Tabulating-Recording Company (CTR). [12] Revenue from being the leading data-services provider to governments around the world helped fuel the company's growth, and in 1922 it was renamed International Business Machines (IBM). [13]

The world-wide depression that began in late 1929 escalated the demand for government welfare services in every country in the world. The computers of the day were the only means available to do such things as count the number of unemployed, to determine the size of their families, and to determine the amount of their benefits.

Within weeks after Hitler came to power in January 1933, for example, IBM began investing millions of Reichsmarks to expand the manufacturing capacity of its German division (Dehomag). The company considered it a safe bet since it anticipated a significant growth in business due to the Nazi's well-publicized desire to increase monitoring of the German people. [14] IBM handsomely profited by modifying its equipment so it would be more useful to the Nazi government's data compilation and analysis objectives, and from selling it the more than *4 million* punch cards it used daily. [15]

Mirroring the growth in computer services in Germany was the dramatically increased demand in the U.S. following President Roosevelt's inauguration in January 1933. He pushed for the creation of numerous government programs, such as the National Recovery Act of 1933 that resulted in a huge increase in demand for computer equipment and supplies. [16] The collection of data on Americans again increased with the passage of the Social Security Act of 1935 and the initial assignment of a federal identity number to over twenty-six million of Americans. To handle the work load generated by Congress' creation of the world's most extensive real-time monitoring of a nation's citizens, IBM developed a special high speed electro-mechanical computer known as the 077. [17] The computer made possible the creation of a single centralized registry of names and numbers required by the Social Security Administration.

A person's name became superfluous to the government after their assignment of a unique Social Security number. The *practical* reason for assignment of a number is that while 100 people may be named William Smith Jones, none would share the same government identifier. The *psychological* reason for assignment of a number is the dehumanizing effect it has on the human psyche.

Only eleven years after Yevgeny Zamyatin's futuristic 1920 novel *We* was first published in English, the Social Security Act brought to life Zamyatin's vision of a world in which a person's identity was embodied in their government-assigned identifier. [18] Reflecting the American people's new status of being identifiable as a number in a database, the first Social Security benefit checks *were* punch cards, and even today government checks have numbers at the bottom that are reminiscent in appearance of the punch card holes they replaced. [19]

The ability of the electro-mechanical computer to efficiently tabulate and analyze census data and other information about tens of millions of people was the crucial means enabling the German and U.S. governments to dramatically increase privacy invasions and physical intrusions into the lives of their respective populations beginning in the 1930s.

The Nazi's use of computer-analyzed census data to enforce military conscription and round up Jews and other undesirables was reflected by Roosevelt's similar use of 1940 census data to organize the military draft and the round-up of Japanese-Americans for confinement in concentration camps after Pearl Harbor. [20] Computers also aided the war effort of both the Allies and Axis powers by breaking military codes and calculating artillery trajectories. [21]

## The Menace of the Electronic Computer

Just as the federal government's *need* to compile information about Americans drove the commercial development of the electro-mechanical punch card computer, the federal government's growing and continuing *need* to compile information about Americans drove the development of the first commercial electronic computer. In April 1946, the Census Bureau gave a $300,000 deposit to two members of the ENIAC research computer team to begin development of a commercial electronic computer to handle compilation of detailed information about the burgeoning population in the U.S. [22] Named UNIVAC (UNIVersal Automatic Computer), the world’s first commercial electronic computer was delivered to the Census Bureau on March 31, 1951. [23]

The public first became aware of the electronic computer’s awesome ability to analyze large amounts of data when UNIVAC correctly predicted that Dwight D. Eisenhower would win the 1952 Presidential Election over Adlai Stevenson. [24] That demonstration provided solid evidence for thoughtful observers that the dynamic analytical capabilities of an electronic computer were a quantum leap beyond those of an electro-mechanical computer. There was not however, a widely perceived need for electronic computers beyond their function of tracking people for the federal government: by 1956 there were less than two dozen in use throughout the world.

The ways in which the electronic computer has enabled government agencies to compile, readily access, and analyze the most personal information about Americans is so well-known that it is redundant to recount more than a few of them. Since 1935 the Social Security number has become a near universal personal identification number (PIN) for contacts between Americans and the government, banks and utility companies; the FBI has credit, law enforcement contact, and other information about literally all adult Americans in its NCIC (national criminal) database; and all state-issued drivers licenses must comply with federal standards. There are also thousands of specialized databases that federal, state, county and state agencies maintain on the Americans who have contact with them.

The following are just a few of the innumerable examples that can illustrate how computerized databases are fulfilling in bold new ways the omnipresent threat computers have long posed to the obliteration of privacy and liberty. Government monitored cameras panning public area use face recognition software melded to a government database to search for hits between a photographed person and a particular person or someone that fits a profile. Digital cameras tied to state DMV databases photograph the license plates of vehicles approaching the border so Customs agents know the registered owner when the vehicle arrives at the checkpoint. People coming into or leaving the country are computer analyzed against a preconceived profile of a person who might be a security threat or involved in drug trafficking or some other unapproved activity. Portable computers in police cars enable law enforcement officers to instantly find out vehicle information and run a criminal background check on the occupants of a car. In addition, since the late 1980s the five Western governments involved in ECHELON have been using computer technology developed by the NSA to monitor a significant percentage of the world's telephone calls, facsimiles, telexes, and email messages transmitted by satellite. [25]

These and other surveillance activities are enhanced by federal and state agencies sharing their proprietary information databases. [26] A revolution in privacy invasions is also related to the digitization of enormous quantities of federal and state public records that makes them more readily available and easily transportable to casual observers. [27] The people named in those records have until now been able to maintain a modicum of privacy because the records were only available in either paper or magnetic tape form to people interested enough in their content to track them down. There is almost no end to the possible examples of privacy invasion that could be cited – and they are escalating as rapidly as the processing power of the computer is increasing. The gravity of the situation is indicated by the estimate that by 2006 the federal government will be spending *$62 billion* annually on surveillance and recording the private activities of Americans. [28]

However, as great as the invasive presence of the government's computerized monitoring of American's is, the menace of the electronic computer is being enhanced many times over by the joining of its information with private databases to create an all-encompassing surveillance capability. Concepts such as "data mining" and "predictive profiling" are being used to analyze the innumerable public and private electronic tracks in the sand people leave.

The FBI, for example, has purchased data from a national credit reporting agency and mailing list brokers to augment the information in its NCIC database, and it also used that information to create new federal criminal records for tens of millions of Americans. Another example is that after the events of September 11, 2001, a major national supermarket chain voluntarily and covertly turned over to the FBI its database of customers who have a discount club card, and the purchases they had made with their card. [29]

Those events also resulted in the head of Oracle, the world's largest database software company, to offer to set-up a "national database" that would be linked to an array of public and private information sources. [30] That data would be intertwined with iris scans, thumbprints and other personal biometric information, all of which would be accessible through a federally issued digital ID card. That card would make state driver's licenses and social security cards obsolete. What wasn't disclosed in news reports about this proposed database linked national ID card is that

Oracle "was founded to assist the CIA with a database project code-named Oracle, and a quarter of its licensing revenue still comes from federal contracts." [31] So under the guise of performing a magnanimous civic duty, the head of the world's leading computer database company – that has close financial ties to the federal government - offered to be a central participant in the establishment of a national ID system.

The ominous menace to privacy posed by the melding of government and private computer resources is also indicated by the FAA's intention to implement a system that will analyze every airplane passenger's financial history, travel history, criminal history, family history, living arrangements and location, and other bits of personal data. The information will be used to build a real time "predictive profile" of the passenger's probability of causing problems, that will then be compared to a standardized "threat index" to determine if the passenger needs to be targeted for a search and questioning. [32]

Another grave menace to privacy is the computerized monitoring of products. It is apropos that the original concept of bar coding and computerizing product information was inspired by Herman Hollerith's use of punch cards to record individualized personal data. Described by its two graduate student inventors in their 1949 patent application as a *Classifying Apparatus and Method*, the bar code was barely used for several decades. [33] In 1972 one of the bar code's inventors expanded on his original concept while working for IBM, by co-inventing the Uniform Product Code (UPC). Although the UPC fulfilled the initial promise of the bar code as a product cataloguing and tracking tool, it was a market failure. Duplicating the computer's history, there was no rush by private industry to use the UPC. As with the computer, it was the federal government's need for UPC technology that is directly responsible for its ubiquitousness throughout society. On September 1, 1981 the Department of Defense mandated that a UPC had to be on every product purchased by the U.S. military. [34] That mandate effectively meant every common consumer product from chewing gum to televisions to dog food had to be marked with a UPC.

The threat to privacy by the universal branding of products with a computer code became crystal clear with the advent of Auto-ID technology. Developed at MIT, a significant recipient of federal intelligence agency funding, Auto-ID supersedes the UPC code with what is known as the Electronic Product Code (ePC). Auto-ID relies on sophisticated computer technology to brand each individual item – such as the cans in a case of pop – with a unique ePC identifier. This branding is accomplished by imbedding a very low cost microchip transmitter, presently the size of a piece of glitter, in each item. The item can be identified by a scanning device - similar to a UPC reader – or its location can be known at any given time by the transmitter's communication of the items identifying ePC to satellites. [35] The identification feature of *Auto-ID* works optimally when a product is purchased by a method linking it to its purchaser. This occurs when a credit, debit or customer discount card is used. That would also occur if as it has been suggested, a digitized national ID card is designed so it could be used as a universal product purchase card.

However, the grand daddy of all surveillance programs was established by the Department of Defense's Advanced Research Project Agency (DARPA) in early 2002. DARPA created the Information Assurance Office to oversee various surveillance projects, one of which is the Total Information Awareness (TIA). That program is intended to collect, store, extract and analyze every known piece of electronic data on all Americans, and selected people in countries around the world. [36] It is planned for TIA to do that through the multi-pronged approach of processing information and communications electronically and biometrically, in multiple languages, and by using predictive modeling of behavior and probable responses. TIA is envisioned to create an electronic DNA body print of the hundreds of millions of people under its surveillance net.

Initially funded by Congress with a $120 million appropriation authorized at the same time the Homeland Security Act was passed on November 20, 2002, the TIA program is a manifestation of that Act's *Information Analysis and Infrastructure Protection* provision. The processing of many thousands of bits of information in real-time related to each of the hundreds of millions of people the TIA will have under constant surveillance is the most demanding data processing project ever undertaken. Technology developed by IBM as a result of its $290 million dollar contract with the federal government for two supercomputers could satisfy the TIA's need for processing power. Announced the day before the Homeland Security Act was passed by Congress, the first of those computers will be 10 times faster than any previous computer, and capable of 360 *trillion* mathematical operations a second. [37]

It should be obvious by now that the computer was not invented so that word processing could replace typing a letter with a typewriter, or so a company's sales could be analyzed with a spreadsheet instead of on graph paper, or so customer information could be compiled in a database instead of keeping track of them with index cards, or so people could email messages instead of making telephone calls. As Jerry Mander observed *In the Absence of the Sacred,* it is arguable that the glamorization and consumerization of the computer has aided the public's acceptance of technology that is fundamentally repugnant to mankind in its purpose. The computers repugnancy is inherent in its *form* of collecting, storing, analyzing and distributing detailed personal information that fulfills its *function* of being an efficient tool for the government to more thoroughly invade the privacy of individual human beings.

## The Menace of the Internet

Although the Internet is generally hailed as a communication and research "wunderkind," the truth is far more disturbing.

For untold millions of people the Internet is considered nearly synonymous with the use of computers. That status makes its origin as a child of the federal government particularly relevant to the tidal wave of privacy invasions occurring in this country and throughout the world. As disturbing as it is that the electro-mechanical and the electronic computer were developed as commercial products to track Americans, it is perhaps more disquieting that the Internet is a child of the military's desire to have a bomb-proof reliable communications network between critical locations during and after a nuclear war. [38]

Development of what evolved into the Internet was begun by the Department of Defense's ARPA in late 1962 (renamed DARPA in 1996). [39] Years of developmental work paid off when data was successfully transmitted by the project in 1969. Initially known as ARPANET - a combination of ARPA and NETwork - the term Internet wasn't used to describe the computerized transmission system until 1982. [40]

The Internet's conception and design as a tool to make nuclear war practical was consistent with the first use of the federally funded ENIAC electronic computer after its completion in December 1945: the design of more efficient nuclear weapons. [41] As previously noted, two of the ENIAC's developers contracted with the Census Bureau to develop UNIVAC, that in 1951 became the first commercial electronic computer.

The probable destruction of telephone lines and intermediate sites during a nuclear war is what led to development of the Internet's unique capability to route information through its network of connections by alternate lines if the most direct route is unavailable. If Omaha and St. Louis are nuked, for example, then data could be routed through Minneapolis, New Orleans, or another routing equipment location. So that aspect of the Internet's form followed its function of making nuclear war a viable military option worthy of serious consideration. The Internet was intended to make the lunacy of the government's policy of Mutual Assured Destruction (MAD) possible. Coincidentally, shortly after the Cuban missile crisis in October 1962 brought the U.S. And Russia to the brink of nuclear war, production began on Stanley Kubrick's Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb, and the military began development of the Internet.

[42]

In addition, since it was designed as a method of transmitting highly classified military information that needed to be authenticated by the receiving party, the capability of ascertaining the source of all messages was incorporated into the Internet's design. That means a backdoor method for monitoring all Internet traffic is a feature of the system. Consequently the Internet's form also follows its function of needing to compromise the privacy of those who use the system.

The success of the military's ARPA networking project in achieving what it was designed for is unknown to the vast majority of people, who simply think of the Internet as a recreational vehicle, a business, shopping, dating or research aid, or an easier or cheaper way to communicate for pleasure or profit. Those benefits are merely incidental to the Internet's purpose of facilitating reliable military and other government communications in a time of great tumult and crisis. Although the military relies on the Internet for well over 50% of its communication, that primary function of the system is outside the public's consciousness due to the government's use of technology inaccessible to the civilian population. [43]

The structure of the Internet also makes it possible for the government to impair the privacy of its users. The government regularly and frequently uses subpoenas, search warrants and intimidation to acquire email logs and messages from Internet service providers, such as AOL. Those companies retain such records even after a person has deleted them from their own hard drive and made them inaccessible to their own email software. Such invasions of privacy are only one aspect of the surveillance made possible by the Internet's extension of the electronic computer's innate qualities, and the melding of private and government databases to create a covertly supra personal information resource.

## The Computer's Menace to Privacy and Liberty

Different aspects of the computer's menace to privacy and human liberty have been explored in various forums. Three of those significant threats are graphically illustrated in a book, a movie and a television series episode that are all more than 30 years old. They reflect the concern expressed by learned people about the possible negative impact of computers to humankind: a concern that seemed to largely evaporate after the 1960s.

*Year of Consent*, a 1954 novella by Kendell Foster Crossen, presents a remarkably accurate vision of the menace electronic computer's pose for the obliteration of human privacy and the submergence of liberty to the whims of rulers exercising near absolute power masked by a public facade of governmental benevolence and concern for carrying out their Constitutional mandates to protect the public's welfare and ensure national security. Crossen's vision includes an extremely powerful central computer that uses predictive software and an enormous database of personal information to electro-biometrically analyze images captured by cameras placed in all public and many private areas to determine who may be thinking thoughts that could threaten the rule of the government. As it is envisioned the Department of Defense's TIA program will bring Crossen's prophecy into the realm of reality.

The 1969 movie, *Colossus: The Forbin Project*, based on D. F. Jones' 1966 book, extended the concept of computer-monitored surveillance to encompass the entire world. It is so intensely real and its vision of the future so disturbing that its release to theaters was delayed until 1970: a year after it was completed. In *Colossus* the catastrophe mankind suffered originated with the government carrying out its mission to provide national security. *Colossus* portrays with crystal clarity how easy it is for the use of electronic devices developed by the government for outwardly benign and beneficently-intentioned purposes to rapidly spin out of control. Multiple aspects of human life were invaded and profoundly affected by the hydra-headed surveillance monster *Colossus* became, and that were unrelated to the stated reasons for its development and deployment.

First broadcast in November 1963, *O.B.I.T.* was an episode of The Outer Limits television series that clearly showed the profoundly negative psychological impact of surveillance systems both on the people being monitored, *and* on the people involved in the monitoring. A murder investigation at a top secret defense facility uncovers the existence of an electronic device called the Outer Bank Individuated Teletracer (O.B.I.T.). O.B.I.T. is capable of spying on anyone at anytime, anywhere, and it is used at the defense facility to help ensure national security. It is learned during the course of the investigation, however, that O.B.I.T. machines have been distributed throughout government agencies and private businesses by aliens who understand the demoralizing impact that spying and being spied on has on the human psyche. O.B.I.T. may have been a prophetic foretelling of the psychological consequences of the escalating level of computerized monitoring and diminishment of privacy in the U.S. and other westernized nations. It also served as a dire warning that pervasive electronic monitoring of human beings is an *unnatural* "alien" process that negatively and perhaps permanently alters the consciousness of the watcher *and* the watched.

Driven by the needs of the federal government, the electronic computer is the vehicle that has enabled the theory and fears of pervasive surveillance to be translated into real life. Reminiscent of O.B.I.T.'s distribution process, the Department of Defense's secretive and mysterious ARPA funnels its technological breakthroughs involving surveillance of Americans into the "private" sector for mass manufacture and distribution. [44]

Proponents of privacy invasions are fond of flippantly asserting that if you have nothing to hide you have nothing to fear from government surveillance and data collection. Yet it is doubtful any of those people believes what they are saying. Their hypocrisy can easily be revealed by proposing that multiple video cameras broadcasting a picture and sound live over the Internet be installed in every room of their home. The cameras would be strategically aimed so people all over the world would be able to view and hear what goes on in every nook and cranny of their home at all times. A person claiming to have nothing to hide would be watched by people all over the world as he or she used the toilet, took a shower or bath, changed their clothes, brushed their teeth, as well as everything else they did in their home. People worldwide would know what brand of breakfast cereal the person ate, whether they chewed with their mouth open, what brand of deodorant they used, how often they changed their underwear, and whether they snored.

Portable cameras broadcasting live over the Internet could continue the monitoring of the person's life whenever he or she left their home. People around the world could watch and hear them as they shopped at the supermarket, serviced their car, worked at their job, went to a movie, visited family or friends, or went to a restaurant for Sunday brunch. Is their any doubt every person claiming they have nothing to hide would recoil in horror when faced with having *every* moment of their life watched 24-hours a day by Peeping Toms, government agents and other voyeurs over the Internet?

The technology exists for a person to live a real life O.B.I.T. situation that would have profound psychic effects on not just that person's mind and behavior, but on the watchers as well. It may even be the case that living inside an all-pervasive surveillance prison 24-hours a day can be more psychologically debilitating than confinement in a physical prison where moments of privacy may be found occasionally. [45]

Humanity thus faces ever-increasing privacy invasions that are indicative of the computer's continuing fulfillment of its function and purpose for being. From whatever perspective one looks at Herman Hollerith's invention, his success at creating a comprehensive instrument of human monitoring makes him the Godfather of the modern surveillance state.

There is a German word describing what Hollerith hath wrot on mankind: *Karteimensch*, which loosely means the living of a punch card existence. Every person in a society dominated by computers has a digital representation of their life stored in multiple databases. Insofar as those who rely on those databases for information about the person are concerned, the person's existence is not defined by who they are as a person, but by how they are categorized in those databases. So the more a society relies on computers, the more the people in that society can be considered to live “a punch card existence.”

Compounding moral and philosophical issues related to replacing the evaluation of a person based on who they actually are with a numerical representation of them that exists only in an inanimate database, is the consideration that it is known computer databases have a high degree of erroneous and stale data. [46] So any computer based punch card representation of a person is likely to be seriously flawed.

In spite of the electronic computer’s inherent deficiency in generating unreliable results from data that is inaccurate at the time it is accessed, it has fueled the growth of modern machine-like bureaucratic structures engaging in a level of monitoring previously unknown in human history. Its latent menace is indicated by the Nazi’s reliance on primitive computer punch card technology to shower a reign of terror on tens of millions of people.

Given the current extent of data collection and surveillance, considerations of a national ID card in the U.S. are more symbolic than substantive. The national ID card would be a front-end for accessing information already accumulated by a multitude of current data-collection methods. However, a national ID card would also endanger people by providing more ready access to that information. In 1890, a far-seeing person could have likely predicted that some form of national ID card would one day be a reality. Such an ID card is simply an extension of the surveillance capabilities of Hollerith’s original electro-mechanical computer. [47]

The all-pervasive presence in our society is the direct result of the federal government’s Constitutional mandate to use the Census Bureau to spy on American’s every 10 years. If the federal government had not spurred its invention, commercial marketing and continued development, the computer as we know it today would not exist. [48] In many cases private users have taken advantage of the computer’s integrated spy capabilities to mimic the government’s use of them as an invasive personal data resource. However, if perchance the computer had been invented under alternate circumstances for private uses unrelated to invading privacy, it would be at a different stage of development and its form would likely be radically different. It is even less likely the Internet would exist in the absence of the federal government's need for its creation, since there is no need in the private world corresponding to the military’s push for its development to ensure reliable and secure communications during a nuclear war.

This means the benign uses of computers by individuals and businesses are only incidental to their central function of *spying* on people, and those relatively innocuous uses obfuscate reality by creating the illusion that the *spying* is the incidental activity. The perceived and trumpeted advantages of using the computer and its child - the Internet – misdirect attention away from the deviousness underlying it like a Siren's song lured enchanted mariners to their deaths on hidden rocks.

The multitude of invasive purposes computers are being used for today does not stem from the misuse of a neutral technology. Quite to the contrary, those *nefarious* uses are the most perfect expression of the technology underlying the conception and design of computers. That emphasizes a great unresolved issue facing humanity: How is it to deal with the fundamental nature of the computer as a device created for the efficient destruction of privacy, and concomitantly, human liberty?

## Conclusion

Our liberty has been subverted by the avalanche of privacy invasions that have followed in the wake of the computers invention as a means of turning the census into a gold mine of detailed information about Americans.

The degree to which our liberty has evaporated in the face of seemingly beneficent public and private computerization is not surprising to those who understand its relationship to privacy. One hundred and twenty-seven years before Herman Hollerith had his "ah ha" moment of conceiving the computer that changed the world, William Thornton expressed his fears to the House of Commons about the consequences of surveilling the British people with a census: "I hold this project to be totally subversive of the last remains of English liberty." [49]

In his 1851 book, *Idee Generale de la Revolution au XIX Siecle* , Pierre-Joseph Proudhon gave voice to what Thornton left unspoken: A census is destructive to liberty because it contributes to a person being, "…. noted, registered, enumerated, accounted for, stamped, measured, classified, audited, patented, licensed, authorized, ... in every operation, every transaction, every movement." [50] Those are the very activities the computer has enabled to be done to a degree that was only imaginable before its creation.

The proclamation of the lead character in the 1967-68 television series *The Prisoner*, who was imprisoned in a remote village, designated as Number 6 and subjected to omnipresent electronic and human surveillance may prove to be an anthem for those of the 21st Century that cherish liberty: "I am not a number. I am a free man! I will not be pushed, filed, indexed, debriefed, or numbered!" [51]

That emphatic statement sums up the intertwining relationship between privacy and liberty: the former is a prerequisite for the latter. Envisioned and designed to obliterate privacy, the computer is doing the same to liberty. Man is now left to ponder how to deal with the consequences of what Herman Hollerith loosened upon the world: a grave menace to human liberty. [52]

It is not a problem that can be ignored except at our peril, because whether one's life is scrutinized and cataloged under the guise of a census, a bank account number, a social security number, a supermarket discount card, or a national identification card, the result is the same: one's liberty is undermined and its exercise impaired.

THE END

Endnotes follow:

[1] December 27, 2002.

[2] Justice Brandeis dissented in *Olmstead v. U.S.*, 277 U.S. 438, 479 (1928). That was the first case in which the Supreme Court gave its stamp of approval to the wire tapping of private telephone conversations by government agents. Justice Brandeis wrote: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, *the right to be let alone – the most comprehensive of rights and the right most valued by civilized men.*" (emphasis added)

[3] *Article I, Section 2*. One of the two specific purposes of the census provision was to facilitate tax collection.

[4] *IBM and the Holocaust*, Edwin Black, Crown Publishers, NY, 2001, 25.

[5] *IBM: Colossus in Transition*, Robert Sober, Truman Talley Books, NY, 1981, 14, cited in *IBM and the Holocaust* at 25 fn.5.

[6] One of these was the Schertz calculating machine, circa 1855.

[7] *Building IBM: Shaping an Industry and Its Technology*, Emerson W. Pugh, MIT Press, Cambridge, 1995, 12-13, cited in *IBM and the Holocaust*, 26 fn. 10.

[8] *IBM and the Holocaust*, 26, 28. The next census in Russia wasn't performed until 1926.

[9] *Id*. at 27

[10] *Id*. at 26

[11] *Psychological Principles in System Development*, Robert M. Gagne' and others, Holt, Rinehart and Winston, N. Y., 1966, 78. It is also noted in the book that the punch cards were referred to as Hollerith cards after their inventor.

[12] *IBM and the Holocaust* at 31.

[13] *Id*. at 40

[14] *Id*. at 50. IBM was able to increase its investment in Germany in near secrecy because the name of its German subsidiary, Dehomag, didn't imply any connection with IBM. For the same reason, IBM was able to export American computer technology to Germany that the company profited from by servicing the needs of the Nazis.

Dehomag was founded in Germany in 1910 to market Hollerith's machines in exchange for a share of its business and royalties on his patents. *Id*. at 30. IBM assumed 90% ownership of Dehomag in 1922 when it became an IBM subsidiary. *Id*. at 43.

IBM's aiding of the Nazis in their cause without any moral compunction dated back to the precedent Hollerith set in the mid 1890s when his fledging company performed a census of Russia that could have provided information to be used by Czar Nicholas II to strengthen his rule. *Id*. at 46-47.

IBM's moral neutrality about the use of its technology was very financially rewarding. In 1933 its German subsidiary, Dehomag, generated over 50% of the profits of IBM's 70+ foreign subsidiaries. *Id*. at 43-44. Dehomag has been known as IBM Germany since 1971.

[15] *Id*. at 22

[16] *Id*. at 46

[17] *Some Computer History*, William Moseley, Ph.D., Interdisciplinary 15, UC Santa Barbara, April 3, 2002, p. 18 at: http://www.ic.ucsb.edu/~int15/lectures/lecture2_s02.pdf.

[18] It is noteworthy that Zamyatin intuitively recognized the relationship between a government assigned number and the utter obliteration of privacy. The two central features of his futuristic vision was the universal use of a government assigned number that replaced the use of personal names in daily activities, and homes that had glass walls so a person was constantly under surveillance by neighbors and passersby. Augmenting the lack of privacy was the inculcation in people from an early age that it was their civic duty to report suspicious activity by strangers, or odd behavior by someone they knew, to the police.

[19] *Id.*

[20] *IBM and the Holocaust* at 344-346. In a radio address encouraging participation in the 1940 census, Eleanor Roosevelt described it as "the greatest assemblage of facts ever collected by any people about the things that affect their welfare." at 345. That information was subsequently used to ghettoize Japanese-American undesirables in concentration camps who also had their wealth confiscated – just as the Nazi's did to Jews, Gypsies, communists and other groups.

[21] Id. at 120. IBM received so many lucrative contracts from the United States government ("from the Department of Labor to the War Department") that "[t]he company became [a] quasi-governmental" entity.

[22] *The History of the UNIVAC Computer – Inventors Presper Eckert and John Machly*, in *Inventors of the Modern Computer*, Mary Bellis, at http://inventors.about.com/library/weekly/aa062398.htm. The ENIAC was a federally funded research computer that when completed in December 1945, was first used to design nuclear weapons and calculate artillery trajectories. Source: Museum of Computer History, RE-PC, Seattle, WA.

[23] *Id.* The Census Bureau placed a $400,000 ceiling on the project when the computers design and contract was finalized in 1948. Remington Rand, Inc. bailed out Drs. Eckert and Machly when they ran out of money in 1950. The computer was completed by the UNIVAC Division of Remington Rand. A total of forty six UNIVACs were sold to government and large businesses.

[24] *Id.*

[25] The transmissions are scanned for the presence of predetermined keywords that could indicate involvement in some covert activity. See e.g., *Secret Power: New Zealand's Role in the International Spy Network*, Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, 1996. See an excerpt from the book in CovertAction Quarterly at: mediafilter.org/caq/echelon/

[26] *Government Exchange and Merger of Citizens' Personal Data Called "Systematic and Routine,"* privacilla.org, March 12, 2001. Available at: http://www.privacilla.org/releases/press005.html

[27] See e.g., *The End of Practical Obscurity*, privacilla.org, June 15, 2001. Available at: http://www.privacilla.org/government/practicalobscurity.html

[28] *Silicon Valley's Spy Game*, Jeffrey Rosen, NY Times Magazine, April 14, 2002. Available at: http://www.nytimes.com/2002/04/14/magazine/14TECHNO.html

[29] *Store Customer Cards a Source for FBI?*, Kelley Beaucar Vlahos, Fox News, August 1, 2002. See also, CASPIAN's website at www.nocards.com.

[30] As of September 20, 2002, Oracle's annual revenues were $10.8 *billion*. Source: http://www.oracle.com/corporate/index.html

[31] *The Security Traders: as Washington prepares to spend tens of billions on Homeland Security, companies are gearing up for the biggest government bonanza since the Cold War*, Brendan I. Koerner, Mother Jones, October 2002 (6), pp. 46-47.

[32] *Silicon Valley's Spy Game,* Jeffrey Rosen, NY Times Magazine, April 14, 2002.

[33] *Bar Code 1*, Russ Adams, http://adams1.com/pub/russadam/history.html and, *History of Bar Codes*, Tony Seideman, American Heritage of Invention and Technology, reprinted at: http://www.swlamall.com/WebTronics/barcodeHostory.htm

[34] *Id.*

[35] See the official MIT Auto-ID website at: http://autoidcenter.org/main.asp

[36] For an excellent explanation of the implications of the TIA project, see, *You Are A Suspect*, William Safire, The New York Times, Nov. 14, 2002; and, *A Supersnoop's Dream*, Audrey Hudson, The Washington [D.C.] Times Nov. 15, 2002. Mr. Safire didn't mention that state drivers licenses can easily be turned into de facto national I.D. cards by linking them to the TIA databases, and any other database collection and analysis system authorized under Homeland Security's Title II's.

[37] *I.B.M. Plans a Computer That Will Set Power Record*, John Markoff (staff), The New York Times, Technology Section, November 19, 2002. The computer is code named Blue Gene/L. The publicly announced purpose of the supercomputers is to do simulations related to nuclear war and nuclear waste. However, just as the development of the ENIAC computer in 1945 that was used for nuclear weapons related research, led to development of the UNIVAC for the Census Bureau, the technology underlying the Blue Gene/L will enable a level of data processing that was inconceivable prior to its development.

[38] *A Brief History of the Internet*, Walt Howe, April 21, 2002. Available at: http://www.walthowe.com/navnet/history.html .

[39] *Hobbes' Internet Timeline v5.6*, Robert H Zakon, April 1, 2002, Available at: http://www.zakon.org/robert/internet/timeline/. The Defense Department formed ARPA in 1958 after the Russian's launched the Sputnik satellite, to ensure the U.S. would have the lead in militarily useful science and technology. DARPA is independent from other military R&D agencies and it reports directly to senior DoD officials.

[40] *A Brief History of the Internet*, Walt Howe, April 21, 2002. Available at: http://www.walthowe.com/navnet/history.html . ARPA (also known as DARPA) is still the central military research organization. See: www.darpa.mil .

[41] *The History of the UNIVAC Computer*, supra. The ENIAC was a federally funded research computer that when completed in December 1945, was first used to design nuclear weapons and calculate artillery trajectories. Source: Museum of Computer History, RE-PC, Seattle, WA.

[42] Source: http://www.teachwithmovies.org/guides/dr-strangelove.html

[43] *The ARAPANET*, Professor Peter Kirstein, June 26, 1998. Available at: http://www.funet.fi/index/FUNET/history/internet/en/1980.html . This technology includes sophisticated encryption technology.

[44] See e.g., A summary of DARPA's mission and accomplishments on its website at: www.darpa.mil/body/pdf/transition.pdf .

[45] O.B.I.T.'s all pervasive monitoring is an extension of Jeremy Bentham's idea of a Panoptical Prison constructed so that all prisoners would be subjected to near constant surveillance.

[46] See e.g., *The Justice Juggernaut: Fighting Street Crime, Controlling Citizens*, Rutgers University Press, New Brunswick, 1991. pp. 70-75.

[47] The ghost of Herman Hollerith lives on in IBM's recent development of a computer storage device code named Millipede that stores information by punching tiny holes in a plastic surface. Resembling a tiny punch-card system, Millipede stores data at a density 20 times more than the most advanced magnetic or electronic devices. Millipedes indentations can be erased and rewritten hundreds of thousands of times, and its nanotechnology can pack 3 billion bits of information into a hole the size of that used to store a single bit of information in the Hollerith's original computer. That translates into the storage of 25 million pages of data on a surface the size of a postage stamp. Source: *IBM Updates Punch-Card Storage*, David Legard (IDG News Service), PC World, June 11, 2002.

[48] An excellent indicator that private investors and companies would not have funded the production and marketing of the computer in the absence of the government's involvement is that they *didn't*. Herman Hollerith successfully demonstrated the computer he developed in 1884 to a number of companies, *none* of which purchased a single one. The same computer those companies didn't purchase was the one that the U.S. Census Bureau chose to use for the 1890 census. It was the money from that contract that enabled Hollerith to begin manufacturing his computers. Furthermore, five years after the UNIVAC computer became commercially available, less than *two dozen* were sold worldwide.

Another indicator of why the computer would not have developed as it has in the absence of the government's involvement is that there wasn't, and may still not be a discernable need for them apart from its indisputable ability to compile, store and analyze enormous amounts of data about people. Articles in the Atlantic Monthly have raised the spectre that the computer does not contribute to the productivity of businesses (*The Computer and the Economy; will information technology ever produce the productivity gains that were predicted?* by Alan S. Blinder and Richard E. Quandt, Dec. 1997, v280, n6, p26(6)), and it may even retard the learning of children (*The Computer Delusion*, Todd Oppenheimer, July 1997, v280, n1, p45(14)).

[49] In his 1753 address William Thornton said: "I was never more astonished and alarmed since I had the honour to sit in this House [...]. And what purpose will it answer to know where the kingdom is crowded [...] except we are to be driven [...] as graziers do cattle? As to myself, I hold this project to be totally subversive of the last remains of English liberty." Process re-engineering: a brief history of Government computing, Kevin Ashley, NDAD Newsletter #8, June 2000. Available at: http://ndad.ulcc.ac.uk/events/newsletters/news008/adros.html

[50] Documenting Individual Identity, edited by Jane Caplan and John Torpey, Princeton University Press, Princeton, 2001, cited at p. 1. A more complete quote is: "To be governed is to be under surveillance, inspected, spied on, superintended, regulated, restrained, indoctrinated, preached at, controlled, appraised, assessed, censored, commanded. ...

To be governed is to be noted, registered, enumerated, accounted for, stamped, measured, classified, audited, patented, licensed, authorized, ... in every operation, every transaction, every movement."

[51] Apropos to this essays theme that a punch card society has been systematically and deliberately created by the federal government is the following question by The Prisoner's lead character, and the response by his captors: "What do you want?," to which they respond, "We want information, and by hook or by crook we will get it!"

[52] This begs a disturbing question to be asked and the answer needs to be faced clearly. Since it was known by learned people at the time the Constitution was written that one of the most destructive acts the government could take to undermine human liberty was a census, why was the Constitution written to mandate a national census every 10 years? In other words, the "founding fathers" specifically included the obliteration of privacy and the accompanying destruction of liberty is a built-in feature of the Constitution. For that reason alone the Constitution cannot be viewed as a document promoting human liberty. It was left to Herman Hollerith to create the technology that enabled the effects of the census mandate, which can be referred to as the "liberty destruction provision," to be fully realized.