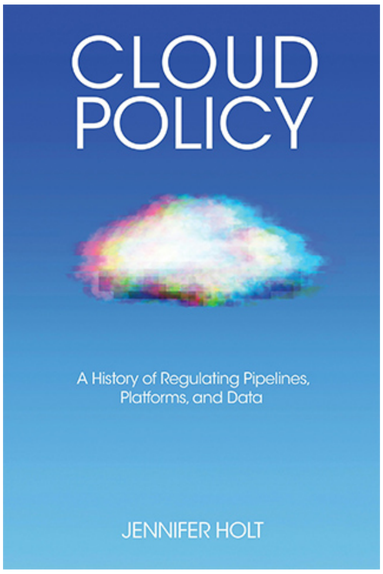
# 60 Years Ago, Congress Warned Us About the Surveillance State. What Happened?

The MIT Press Reader ⋮ 18-23 minutes ⋮ 9/27/2024

"We must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return."

RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS
RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS
RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS

*In the 1960s, Congress turned the tables and began to address the threat that the state and its use of computerized technologies posed to the privacy of its citizens. Much of this was in response to President Johnson's proposal for a "National Data Center" in 1965 to consolidate federal databases as part of the Great Society project. Congress became alarmed and held numerous hearings in the House and Senate between 1966 and 1967 to discuss the many potential invasions of privacy represented by government control of individual data. The idea of a state repository of citizen data created quite an uproar, as explored in the text that follows, and the "National Data Center" did not come to pass.*



This article is excerpted from Jennifer Holt's book "Cloud Policy." An open access edition of the book can be freely downloaded here.

*A decade later, in 1975, the Church Committee, chaired by Senator Frank Church, convened to investigate widespread intelligence abuses by federal agencies, including the CIA, FBI, NSA, and IRS. Prompted by whistleblower Christopher Pyle's exposé of the Army's domestic surveillance, the committee revealed extensive government spying on American citizens, often based on political beliefs with no link to violence or foreign threats. In a chilling interview on Meet the Press that summer, Church amplified his warnings, pointing to "a future in which technological advances could be turned around on the American people and used to facilitate a system of government surveillance." If the U.S. continued down this path, he cautioned, "No American would have any privacy left," emphasizing that "we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return."*

---

Cultural fears about the state's ability to track its citizens have circulated at least since the 1930s when the New Deal ushered in Social Security and a panic ensued over being assigned an identification number that would follow one all the way to the grave. These fears continued through the 1950s with the Red Scare, loyalty oaths, and the anti-Communist crusades of the House Committee on Un-American Activities. However, Congress did not devote much attention to the privacy of individual citizens until the 1960s, when concerns reached new heights, thanks in part to technological advances.

Portable recording technologies and computing began to sound alarms, as their capabilities elicited new threats to privacy rights. Such worries were amplified by the Supreme Court, as Chief Justice Earl Warren stated in a 1963 opinion regarding recording devices and entrapment: "The fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual." In addition, a wave of writing by scholars and journalists at this time, focused on technology, privacy, and personal autonomy, helped inform public debate. In many ways this work anticipated current anxieties about the price of life under Big Tech.

In many ways this work anticipated current anxieties about the price of life under Big Tech.

Vance Packard's "The Naked Society" (1964), Alan F. Westin's "Privacy and Freedom" (1967), and Arthur Miller's "The Assault on Privacy" (1971) were among the most influential in this genre. Miller understood then that the time would soon come when "our primary source of knowledge will be electronic information nodes or communications centers located in our homes, schools, and offices that are connected to international, national, regional, and local computer-based data networks." Westin evoked many present-day issues in his wide-ranging, foundational book, paying great attention to "data surveillance" and how new technologies were affecting norms of privacy in order to recuperate this "cornerstone of the American system of liberty." He viewed privacy and freedom as inextricably linked, defining privacy as "the claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others." "Privacy and Freedom" is still useful today for thinking about the malleable parameters of privacy, and its power in defining an individual's relationship to the state.

This was the context in which President Lyndon B. Johnson proposed a federally controlled data center called the National Data Bank in 1965 as part of the Great Society project. The data center was imagined as a tool for efficiency and organization that would consolidate federal databases at the dawn of computerized record-keeping. However, concerns about technology and privacy were becoming widespread enough that a congressional Special Subcommittee on the Invasion of Privacy was established in the House of Representatives. Four separate hearings were held in the House and Senate between 1966 and 1967 to discuss the threats to privacy posed by the computer and the government control of data. They were dominated by overwhelming expressions of concern about the sanctity of individual privacy and civil liberties. The government's power combined with the yet-unknown capabilities of digital technology were positioned as the main potential threat. The determination that the public needed to be protected from the centralized state collection of data above all else, without sufficient attention to the dangers lurking elsewhere, was a defining moment for cloud policy that has only grown more consequential over the decades that followed.

The chair of the Subcommittee on the Invasion of Privacy running the House hearings, Representative Cornelius "Neil" Gallagher (D-NJ), introduced the investigation of the National Data Center in July 1966 by saying, "The possible future storage and regrouping of such personal information … strikes at the core of our Judeo-Christian concept of 'forgive and forget,' because the computer neither forgives nor forgets." Representative Frank Horton (R-NY) warned that "the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age.… It is not enough to say 'It can't happen here'; our grandfathers said that about television." One of the original network architects of the Internet, Paul Baran, alluded to threats posed by the future cloud in his expert-witness testimony, noting that "a multiplicity of large, remote-access computer systems, if interconnected, can pose the danger of loss of the individual's right to privacy — as we know it today." Author Vance Packard called attention to the "suffocating sense of surveillance" engendered by a centralized government database, noting the "hazard of permitting so much power to rest in the hands of the people in a position to push computer buttons, … [because] we all to some extent fall under the control of the machine's managers."

Gallagher had a remarkably prescient grasp of technological threats to individual privacy, which was likely a result of being persecuted and having his own privacy violated for many years by J. Edgar Hoover and the FBI. Gallagher's speech to the American Bar Association in 1967, titled "Technology and Freedom," was quite striking in its predictive accuracy. It included the following, partially adapted from the statement of Professor Arthur Miller at the Senate hearings that same year:

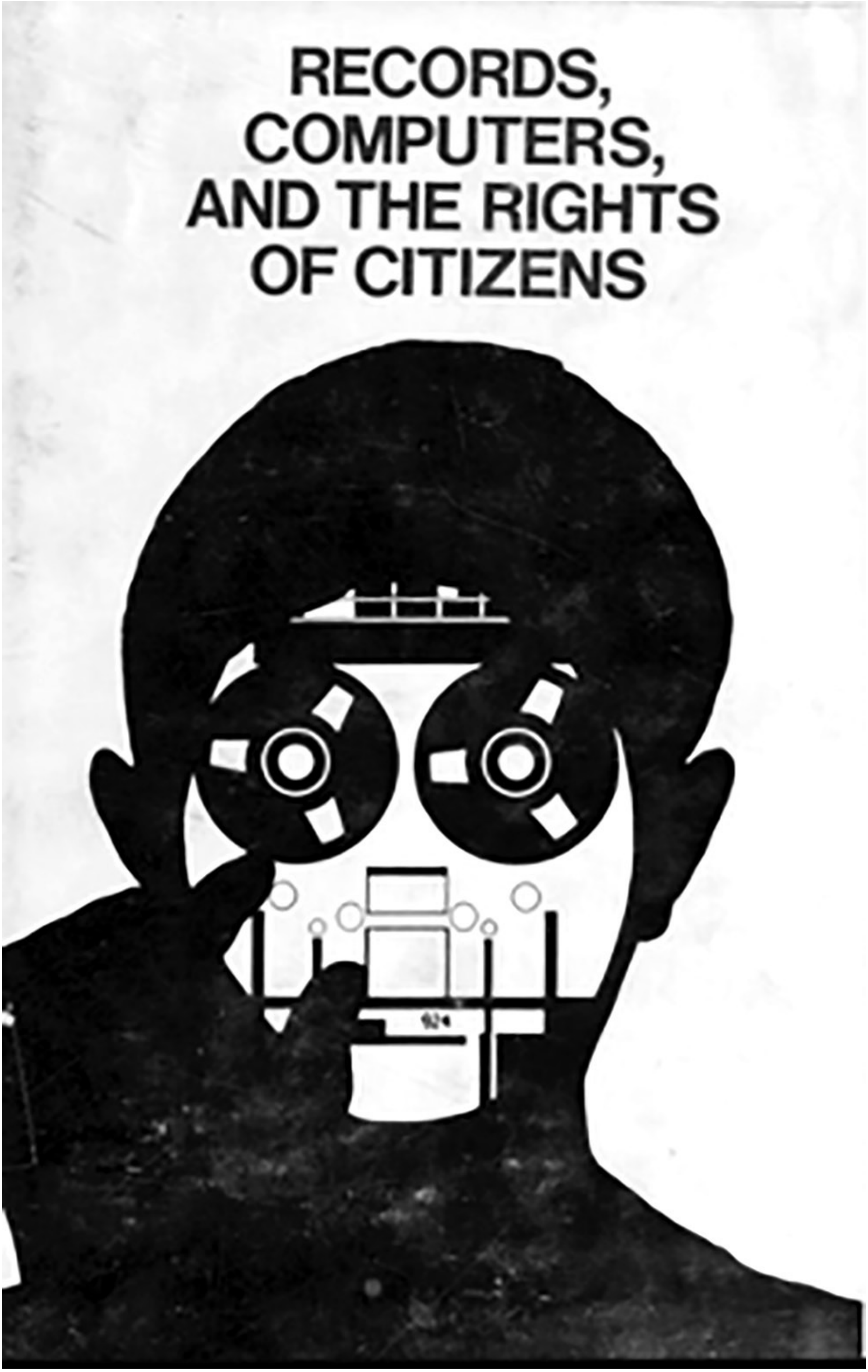
> Although the technology of computerization has raised new horizons of progress, it also brings with it grave dangers.… The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer. If information is power, then real power and its inherent threat to the Republic will not rest in some elected officials or Army generals, but in a few overzealous members of a bureaucratic elite.

The final report from the House Committee was clear about the links between data privacy and democracy: “A suffocating sense of surveillance, represented by instantaneously retrievable, derogatory or noncontextual data, is not an atmosphere in which freedom can long survive,” the authors wrote. “This report, therefore, charges the Federal Government as well as the computer community with a dual responsibility.… They must … guarantee Americans that the tonic of high speed information handling does not contain a toxic which will kill privacy.” The committee further noted that the dangers of unauthorized access to information was great, and “a grave threat to the constitutional guarantees exists in the National Data Bank concept,” leading to their emphasis on prioritizing privacy in the center’s eventual design and implementation. However, the committee’s ultimate recommendation was to stop working on the National Data Bank until privacy protections were fully explored and guaranteed “to the greatest extent possible to the citizens whose personal records would form its information base.” Once again linking privacy to politics, the authors emphasized, “While computerized data bases hold great promise, they must contain procedures which can assure the continuation of freedom of thought and action that is such a vital part of the American tradition. The collection and processing of statistical data should not and need not be gained by sacrificing the guiding principles of our democracy.”

*From the November 1967 cover of the Atlantic. Credit: Drawing by Edward Sorel.*

At the same time, the reporting in the popular press was highly alarmist. One representative article in *Look* magazine titled “The Computer Data Bank: Will It Kill Your Freedom?” posed various questions that could easily be answered by “any snooper with a computer,” such as, “Did your sister have an illegitimate baby when she was 15? Did you fail math in junior high? Are you divorced or living in a common-law relationship? Do you pay your bills promptly? Are you willing to talk to salesmen? Have you been treated for a venereal disease? Are you visiting a psychiatrist? Were you ever arrested?” Chairman Gallagher was quoted in the same article, warning, “Computer data banks are at the same stage of development as the early railroads and the first telephone companies, which took a number of years to link themselves together in a nationwide network. Welfare departments, credit bureaus, hospitals, police departments and dozens of other institutions are putting their files into hundreds of relatively small data centers. No matter what you call them, they're still data centers, and they can be linked." The public uproar in response to all these developments led to National Data Bank discussions and debate being shut down by 1970.

Unfortunately, it would be a pyrrhic victory. The focus on protecting public data from the perceived dangers of centralized state collection and storage blinded legislators to the problems created by the solution: putting data in the hands of private companies. Corporations ultimately filled the vacuum created by the National Data Bank's failure, and became the chief custodians of U.S. citizens' private data. As the historian Margaret O'Mara has argued, these decisions actually created the very problem they were trying to prevent. "The privacy warriors of the 1960s would have been astounded by what the tech industry has become. They would be more amazed to realize that the policy choices they made back then — to demand data transparency rather than limit data collection, and to legislate the behavior of government but not private industry — enabled today's tech giants to become as large and powerful as they are." The congressional attempt to defend US citizens from experiencing "big brother" and the world as imagined in Orwell's "1984," which were mentioned relentlessly during the hearings, ended up creating exactly what they were trying to avoid, albeit serving a different master. This is not to suggest that government control over public data is preferable, but instead to emphasize that private control without regulatory oversight has proven to be undeniably disastrous for individual and collective privacy, and a signature failure of contemporary cloud policy. To his credit, Senator Long (D-MO) who presided over the Senate hearings in 1966 and 1967 did warn that if the proposals for a National Data Bank "concerned themselves only with Government interests, and if individual, private interests were ignored, we might be creating a form of Frankenstein monster," but his words went unheeded.



*The report of the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems, 1973.*

The cultural tensions around surveillance lingered, as evident in the 1973 report, *Records, Computers, and the Rights of Citizens*, put out by the Secretary's Advisory Committee of the

Department of Health, Education, and Welfare. This report was about computerized record-keeping, privacy safeguards, and the issue of the social security number. It is a stunning document that catalogs record-keeping practices going back to the Stone Age through the advent of automated systems. It included similar work on computerized record-keeping and privacy being done in Canada, Great Britain, and Sweden. The report also newly identified citizens as “data subjects,” emphasizing privacy safeguards and the individual’s loss of control over the use of their personal data. In so doing, this 1973 report predicted many of the problems created by Big Tech business models, arguing that concerns about computerized records usually center on privacy, particularly as “privacy is considered to entail control by an individual over the uses made of information about him. In many circumstances in modern life an individual must either surrender some of that control or forego the services that an organization provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms.”

The report also recommended a federal “Code of Fair Information Practice,” which contained principles for transparency, autonomy over one’s personal data, and safeguard requirements regarding data usage by third parties. None of these recommendations were adopted at the time. However, they went on to inform future agency recommendations and early privacy legislation such as the Privacy Act of 1974, which was enacted in the wake of President Nixon’s resignation. And yet, as O’Mara has pointed out, much of this legislation concentrated on the right to know about what information that federal databases held, but none of it “addressed the question of whether this information should have been gathered in the first place.” The 1974 act did not stop data collection, it merely revealed how much of it was taking place on the federal level. According to historian and author Sarah Igo, despite being “designed to empower citizens vis-à-vis the record keepers, the law would wind up stoking fears that the United States had become a full-fledged surveillance society in which individuals were outmatched from the outset.”

The 1974 act did not stop data collection, it merely revealed how much of it was taking place on the federal level.

These widespread concerns at the dawn of the computerized era led to yet another round of hearings in the Senate in 1975. This time the focus was on “surveillance technology,” as news had emerged about the Pentagon’s surveillance of Vietnam War protestors, and journalists exposed the Johnson and Nixon administrations for utilizing a computerized, networked domestic spy operation that, the report stated, linked “the CIA, the Defense Intelligence Agency, the National Security Agency, more than 20 universities, and a dozen research centers, like the Rand Corporation.” Echoing the foreboding words of Frank Church issued just a month earlier, Chairman John Tunney (R-CA) opened the hearings saying, “Technological developments are arriving so rapidly and are changing the nature of our society so fundamentally that we are in danger of losing the capacity to shape our own destiny.” He further stated that “control over the technology of surveillance conveys effective control over our privacy, our freedom, and our dignity — in short, control over the most meaningful aspects of our lives as free human beings.” MIT President Jerome Wiesner testified that the surveillance problem had become a crisis because “information technology puts vastly more power into the hands of government and private interests that have the resources to use it” and “to the degree that the Constitution meant for power to be in the hands of the ‘governed,’ widespread collection of personal information poses a threat to the Constitution itself.” Ultimately, Weiser argued that there is “serious danger of creating an ‘information tyranny’ in the innocent pursuit of a more efficient society.” The committee echoed his tone, raising alarm that the “continued ignorance of surveillance technology — its size and structure as a separate industry, the justifications for its growth, its impact on society — could prove to be an Orwellian catastrophe for our privacy and our freedoms.” As it turned out, all of these fears were well-founded. These proceedings contained vital warnings and lessons for the future of cloud policy that have since been lost to history.

In the end, history is always our best teacher. If cloud policy has taught us anything, it is that the same legal and cultural struggles will await the next critical infrastructural technology and the one after that — until the issues they represent are widely understood as those necessary to defend civil liberties and the health and vitality of democracy, and they are regulated accordingly. Sadly, most citizens remain unaware, uninterested, or unsure of what to do about our current predicament. This is in part attributable to a lack of public education about the issues and stakes of cloud policy, to impoverished and compromised political leadership, and to the poor quality of media coverage about the regulation of cloud infrastructure. In turn, the breakdown of public values in this policy domain has snowballed at a truly alarming rate — bringing us ever closer to the “abyss from which there is no return” that we were warned about so many years ago.

---

***Jennifer Holt*** *is Professor and Chair of Film and Media Studies at the University of California, Santa Barbara, and a former Fellow with the Center for Democracy & Technology in Washington, DC. She is coeditor of “The SAGE Handbook of the Digital Media Economy” (Sage) and author of “Empires of Entertainment” (Rutgers University Press) and “Cloud Policy,” from which this article is excerpted. An open access edition of the book can be freely downloaded here.*