UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 86 ● Fall 2024

THE PRIVACY ACT OF 1974: THE AMERICAN BILL OF RIGHTS ON DATA AND ITS UNFINISHED BUSINESS

Dongsheng Zang

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

THE PRIVACY ACT OF 1974: THE AMERICAN BILL OF RIGHTS ON DATA AND ITS UNFINISHED BUSINESS

Dongsheng Zang*

ABSTRACT

In the midst of the artificial intelligence ("AI") revolution and the debates around it in 2023, this Article proposes to revisit the history of the Privacy Act of 1974, a federal statute that attempted to revolutionize the notion of privacy in response to automated data processing in the computer age. By recognizing that an individual should have the right to control data about herself, the 1974 Act went beyond the Warren-Brandeis framework of privacy based on tort law—the 1974 Act was essentially an American Bill of Rights on data.

The Article first tracks the conceptual development of this new idea of privacy by looking into congressional hearings and broad literature in the 1960s and early 1970s when the computer was introduced in federal government agencies. It describes the process from a theory of scholars and activists such as Alan Westin, to a consensus and policy position largely formed around the year 1971. Based on this central thesis, a "code of fair information practice" laid out five fundamental principles (openness, individual access, collection limitation, use and disclosure limitation, and information management) as the foundation for the 1974 Act. The Article then tracks privacy litigation subsequent to the 1974 Act. Here the Article demonstrates that in the decades after its enactment, the Act was substantially undercut in federal courts as the latter insisted on the old-fashioned tort law theory

* Associate Professor of Law, University of Washington School of Law. I wish to thank my colleague Professor Michael W. Hatfield for sharing with me an early edition of his article, *Safeguarding Taxpayer Data*, 26 FLA. TAX REV. (forthcoming 2023). I am indebted to Professor Tatsuhiko Yamamoto of Keio University for inviting me to join his research project on comparative constitutional protection of data privacy. Professor Shigenori Matsui of University of British Columbia kindly shared with me his research on "My Number" in Japan. In the process of working on this Article, I benefited from Professors Daniel H. Foote, Lawrence Repeta, David G. Litt, Jody Chaffe, William S. Bailey, Shannon W. McCormack, Xuan-Thao Nguyen, and Elizabeth Porter for their insights, support, and encouragement.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

in interpreting the Act. Today, the Privacy Act of 1974 largely falls to oblivion—it is barely mentioned in the current debates on AI regulation.

The Article argues that the 1974 Act is an unfinished business not only because of its unfulfilled promises. While struggling at home, the ideas behind the 1974 Act were more successful abroad. This Article shows that the American congressional hearings and ideas behind the 1974 Act stimulated and facilitated first-generation data protection laws across the Atlantic during the 1970s. That central thesis has gained constitutional status in courts in Germany, India, South Korea and Taiwan, through the doctrine of informational self-determination. In the wake of the AI revolution, what we need is to learn from and strengthen the 1974 Act. What we need today is to finish what was left in 1974, and to develop a real American Bill of Rights on data.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Table of Contents

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

INTRODUCTION

The year 2023 witnessed an artificial intelligence ("AI") revolution. On January 23, Microsoft announced that it would invest $10 billion in OpenAI, a San Francisco-based start-up developing a capable chatbot called ChatGPT.[1] On February 7, Microsoft added ChatGPT to its search engine, Bing.[2] On March 21, Google released its own AI tool called Bard.[3] At the Microsoft Build 2023 conference on May 23, Microsoft announced its plans to expand the use of AI across its apps and services, including for Windows and Microsoft Office.[4] In the meantime, warnings of the dangers of AI intensified. On March 22, an open letter signed by Elon Musk and other prominent AI experts was published, calling for all AI labs to immediately pause for at least six months in consideration of the "profound risks to society and humanity."[5] In early May, Geoffrey Hinton, an AI pioneer, quit his job at Google and joined critics in warning the general public of these grave concerns.[6]

In the midst of these conflicting visions and opinions on AI, the U.S. Congress responded with its own probe into the issues. On May 16, 2023, the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law launched the first of a series of hearings.[7] The Senate Subcommittee and its distinguished guests focused

---

[1] Cade Metz & Karen Weise, *Microsoft to Invest $10 Billion in OpenAI, the Creator of ChatGPT*, N.Y. TIMES (Jan. 24, 2023), at B1. Two months before this announcement, OpenAI made the ChatGPT-3 available to the tech circle, and it was well received. *See* Kevin Roose, *The Brilliance and Weirdness of ChatGPT*, N.Y. TIMES (Dec. 9, 2022), at B1.

[2] Cade Metz & Karen Weise, *Microsoft Sets Off a Tech Race With Its A.I.-Assisted Search*, N.Y. TIMES (Feb. 8, 2023), at A1.

[3] Nico Grant & Cade Metz, *With Bard, Google Pulls A.I. Trigger*, N.Y. TIMES (Mar. 22, 2023), at B1.

[4] Emma Roth, *The 5 Biggest Announcements from Microsoft Build 2023*, VERGE (May 23, 2023, (12:54 PM), https://www.theverge.com/23734104/microsoft-build-2023-ai-bing-copilot [https://perma.cc/JFU9-PURN].

[5] *Pause Giant AI Experiments: An Open Letter*, FUTURE OF LIFE INST. (Mar. 22, 2023), https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [https://perma.cc/A2XE-B434]. Elon Musk had his contradictory views on AI. *See* Cade Metz, Ryan Mac & Kate Conger, *Musk's Stance on A.I.: It's Tricky*, N.Y. TIMES (Apr. 28, 2023), at B1.

[6] Cade Metz, *He Warns of Risks from A.I. He Helped Create*, N.Y. TIMES (May 2, 2023), at A1.

[7] *See Oversight of A.I.: Rules for Artificial Intelligence: Hearing Before the Subcomm. on Priv., Tech., & the L. of the S. Comm. on the Judiciary*, 118th Cong. 1st Sess. (2023), S. Hearing 118-37. Senator Richard Blumenthal, Chair of the Subcommittee; Samuel Altman, CEO of OpenAI; Christina Montgomery, Chief Privacy & Trust Officer of IBM; and Professor Gary Marcus, professor emeritus from New York University, were all present at the hearing. *Id.* Subsequent Senate hearings included *Oversight of A.I.: Principles for Regulation: Hearing Before the Subcomm. on Priv., Tech., and the L. of the S. Comm. on the Judiciary*, 118th Cong. 1st Sess. (2023), *Oversight of A.I.: Insiders' Persps.: Hearing Before the*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

on the question of how to regulate AI and what guardrail standards should be established by Congress.[8] On June 22, the U.S. House Committee on Science, Space, and Technology held the first of a series of hearings focusing on AI and innovation, national security, and American leadership in the area.[9] Computer scientists, business leaders, government officials, academics and social groups were invited to share their views. The hearings were live broadcasted and hotly debated on social media. The executive branch acted even more quickly—the Biden Administration published a white paper on AI in October 2022, "Blueprint for an AI Bill of Rights,"[10] which prescribed five fundamental principles, including the principle of data privacy, in response to the concerns of AI.

It seemingly looks normal—American democracy is at work in response to a historic question posed by a looming technological revolution. Upon closer look, however, there must be a sense of déjà vu for historians. Exactly half a century ago, in response to the arrival of the computer, congressional leaders hosted a series of hearings, which led to the enactment of the Privacy Act of 1974 (the "1974 Act"), a federal law that introduced a new notion of privacy in response to automated data processing in the computer age.[11] It was essentially an American Bill of Rights on data, specifically, in connection with the Social Security Number ("SSN"). As will

Subcomm. on Priv., Tech., & the L. of the S. Comm. on the Judiciary, 118th Cong. 1st Sess. (2024), and *The Need to Protect Americans' Privacy and the A.I. Accelerant, Hearing Before the S. Comm. on Com., Sci. and Transp.*, 118th Cong. 1st Sess. (2024) [hereinafter *A.I. Accelerant Hearing*].

[8] Ryan Tracy, *ChatGPT's Sam Altman Warns Congress that AI 'Can Go Quite Wrong,'* WALL ST. J. (May 16, 2023, 1:12 PM), https://www.wsj.com/articles/chatgpts-sam-altman-faces-senate-panel-examining-artificial-intelligence-4bb6942a [https://perma.cc/J55A-SA4N]; Andrew Ross Sorkin, Ravi Mattu, Bernhard Warner, Sarah Kessler, Michael J. de la Merced, Lauren Hirsch & Ephrat Livni, *Washington Confronts the Challenge of Policing A.I.*, N.Y. TIMES (May 17, 2023), https://www.nytimes.com/2023/05/17/business/openai-altman-congress-ai-regulation.html [https://perma.cc/KKN2-8SLW].

[9] *Artificial Intelligence: Advancing Innovation Towards the National Interest, Hearing Before the H. Comm. on Sci., Space, & Tech.*, 118th Cong. (2023). Prior to these hearings, in March 2023, the House Committee on Oversight and Accountability's Subcommittee on Cybersecurity, Information Technology and Government Innovation had hosted a hearing on AI. *See Advances in AI: Are We Ready for a Tech Revolution? Hearing Before the Subcomm. on Cybersecurity, Info. Tech., & Gov't Innovation of the Comm. on Oversight and Accountability*, 118th Cong. 1st Sess. (2023).

[10] OFF. OF SCI. & TECH. POL'Y, THE WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 5–7 (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [https://perma.cc/Z3FG-U5WW] [hereinafter BLUEPRINT]. "You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used." *Id.* at 30.

[11] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a); 5 U.S.C. § 552a.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

be examined in detail, the 1974 Act was proposed, debated, and passed in response to the rise of the computer.[12] In the process, Congress felt the need to go beyond the Warren-Brandeis framework of privacy based on tort law and embraced suggestions from scholars, advocacy groups, and government agencies describing a notion of privacy tailored for the computer age.[13] It centered on the notion of "fair information practices" that gave the data subject some control of the data about herself.[14] Based on this central thesis, the 1974 Act laid out five fundamental principles: openness, individual access, collection limitations, use and disclosure limitations, and information management.[15] The 1974 Act was a revolution in the notion of privacy as it empowered individuals in their relations with government agencies regarding data collection, processing, use, and retention. These principles are still relevant today, probably even more so.[16] However, the 1974 Act itself has faded not only in the public discourse, but also in courtrooms.[17]

This Article aims to revisit the history of the 1974 Act. In the wake of today's AI revolution, what is at stake is not merely history lost to oblivion. We can benefit from reexamining the history of the Privacy Act of 1974 for the following three reasons. First, the 1974 Act was a bold and ambitious attempt to address the issue of privacy. It created a groundbreaking legal framework by empowering individuals who were becoming merely data subjects in the computer age. Congressional leaders like Senator Sam Ervin Jr. campaigned for the new notion of privacy, organized

[12] 5 U.S.C. § 522a; *The Privacy Act of 1974*, ELEC. PRIV. INFO. CTR., https://epic.org/the-privacy-act-of-1974/ [https://perma.cc/ZE9R-CG8J] (last visited Aug. 24, 2024).

[13] *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 147–66 (1973) [hereinafter RECORDS, COMPUTERS, AND RIGHTS REPORT] (listing the individuals and advocacy groups who made presentations to the committee). For discussion of the 1890 article of Samuel Warren and Louis Brandeis, *infra*, see text accompanying note 132.

[14] *Id.*; *Privacy Act*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/footer/privacy-act [https://perma.cc/6P4U-8JJC] (last visited Aug. 29, 2024).

[15] *See infra* Section II.C.

[16] For example, in their testimony before the Senate Committee on Commerce, Science and Transportation, both Professor Ryan Calo and Ms. Amba Kak urged Congress to pass federal law to protect data privacy by embracing principles including data minimization. *See A.I. Accelerant Hearing*, *supra* note 7 (prepared written testimony and statement for the record of Ryan Calo, Professor of Law, University of Washington; prepared written testimony and statement for the record of Amba Kak, Co-Executive Director, AI Now Institute), https://www.commerce.senate.gov/2024/7/the-need-to-protect-americans-privacy-and-the-ai-accelerant [https://perma.cc/AUH3-ENVB].

[17] *See infra* Part III.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

hearings, and collected volumes of congressional hearings accumulated from years of investigation and documentation.[18] The principles behind the 1974 Act may be of heuristic value in the new efforts to address privacy concerns in the age of AI.

Second, the history of the 1974 Act helps us understand the dynamics and institutional barriers of privacy protection in the United States.[19] America's dynamic interaction between civic advocacy, industry, technology, and national politics brought the issue of privacy to Congress, which passed the law. This shows the strength of American democracy and the genius of privacy advocates. However, this American strength is undercut by other elements of its democracy. Congress soon compromised and retreated from the 1974 Act by adding exceptions to the law's data regulation requirements.[20] In the decades following its enactment, the 1974 Act was also severely undercut by federal courts.[21] This was through interpretation of its key sections,[22] as well as a narrow reading of the Constitution which denied constitutional protection to data privacy.[23]

Third, the true value of the 1974 Act cannot be fully assessed without bringing comparative law into the analysis. The 1974 Act was an American-led revolution with a global reach. The congressional hearings (including scholars who testified in those hearings, such as Alan Westin) and the Act itself facilitated and stimulated debates and legislative responses in continental Europe and commonwealth countries during the 1970s and early 1980s.[24] In the following decades, while the 1974 Act was struggling for its survival, the same principles from the 1974 Act were better received in courts and translated into a constitutional doctrine called "informational self-determination" in continental Europe, commonwealth countries, as well as East Asian democracies.[25] In the European Union, the same principles laid the foundation

[18] STAFF OF S. COMM. ON GOV'T OPERATIONS & SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RTS. OF THE H. COMMITTEE ON GOV'T OPERATIONS, 94TH CONG., LEGIS. HIST. OF THE PRIV. ACT OF 1974 S. 3418 (PUB. L. 93-579), at v, 3 (Joint Comm. Print 1976).

[19] *See generally* COLIN J. BENNETT, THE PRIVACY ADVOCATES RESISTING THE SPREAD OF SURVEILLANCE (2008).

[20] *See, e.g.*, 5 U.S.C. § 522a.

[21] *See, e.g.*, Doe v. Chao, 540 U.S. 614 (2004).

[22] *See infra* Section III.A.

[23] *See infra* Section III.B.

[24] *See infra* Part IV.

[25] *See infra* Part IV.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

for the General Data Protection Regulation,[26] and became an integral part of recent legislation, including the Digital Services Act,[27] as well as the proposed Artificial Intelligence Act.[28] For those who believe that privacy is culturally different in America,[29] it is important to retell the story of the 1974 Act to demonstrate that it all started as an *American* revolution modeled on the American Bill of Rights.

In this Article, Part I will cover the rise of the social security number with the introduction of computers in federal governmental agencies in the 1960s. Part II lays out the making of the Privacy Act of 1974. Part III covers litigation during the first decade of the 1974 Act, from 1974 to 1984, and the interpretation of the Constitution on the question of privacy in social security practices. Part IV covers the rise of "informational self-determination" in other countries: continental Europe, commonwealth countries (Great Britain, Canada, Australia, and India), and East Asian democracies (Taiwan, South Korea, and Japan).

I. COMPUTERS, PRIVACY, AND THE SOCIAL SECURITY NUMBER

In the United States, the social security number ("SSN") was the product of the Social Security Act of 1935 (the "1935 Act").[30] The 1935 Act created a Social Security Board,[31] and an "old-age reserve account" in the Treasury Department under the Board for individuals who were entitled to social security benefits.[32] Immigrants, religious groups, and union members became concerned about the account numbers potentially being used for other purposes.[33] The United Mine

[26] Council Regulation 2016/679, 2016 O.J. (L 119) 1.

[27] Council Regulation 2022/2065, 2022 O.J. (L 277) 1.

[28] Proposal for a Regulation of the European Parliament and of the Council on Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 (Apr. 22, 2021).

[29] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153 (2004). For a critique from the viewpoint of German history, see Thomas J. Snyder, *Developing Privacy Rights in Nineteenth-Century Germany: A Choice Between Dignity and Liberty?*, 58 AM. J. LEGAL HIST. 188 (2018).

[30] 42 U.S.C. § 405(b)(2)(B)(i); *see generally* LARRY W. DEWITT, DANIEL BÉLAND & EDWARD D. BERKOWITZ, SOCIAL SECURITY: A DOCUMENTARY HISTORY 83–89 (2008).

[31] Social Security Act, Pub. L. No. 74-271, § 701, 49 Stat. 635, 635–36 (1935).

[32] *Id.* § 201, at 622–23.

[33] ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 284–85 (2000).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Workers and United Steelworkers successfully lobbied the Franklin D. Roosevelt administration to make it possible to replace an existing SSN with a second one.[34] Despite the privacy concerns, "[a]pproximately 30 million applications for SSNs were processed between November 1936 and June 30, 1937."[35] In 1943, President Franklin D. Roosevelt issued Executive Order 9397, making the account number a permanent fixture.[36] In the subsequent two decades, SSNs did not get more attention.[37] This changed in the early 1960s when computers were introduced and installed in federal government agencies.[38]

A. Federal Agencies and the Social Security Number

With the introduction of the computer in the federal government in the late 1950s, "automated data processing" ("ADP") became increasingly employed.[39] The Internal Revenue Service ("IRS") became the champion, pushing for the use of SSNs in 1961.[40] The IRS was soon joined by other agencies such as the Department of the Treasury and the U.S. Civil Service Commission in the use of computer technology in their offices.[41] Increased interest in the new technology prompted proposals for a

[34] *Id.* at 285.

[35] *Social Security Number Chronology*, SOC. SEC. ADMIN., https://www.ssa.gov/history/ssn/ssnchron.html [https://perma.cc/5N6N-8E5R] (last updated Nov. 9, 2005).

[36] Exec. Order No. 9397, 8 Fed. Reg. 16095 (1943). *See generally* MICHAEL P. RICCARDS & CHERYL A. FLAGG, PARTY POLITICS IN THE AGE OF ROOSEVELT: THE MAKING OF MODERN AMERICA (2022) (discussing President Roosevelt's presidency).

[37] On two occasions, the United States Supreme Court was asked to consider the Social Security Act: in *United States v. Murdock*, 284 U.S. 141 (1931), and in *Shapiro v. United States*, 335 U.S. 1 (1948).

[38] *See, e.g.*, *Plans for Taking the 1960 Census: Hearing Before the Subcomm. on Census & Gov't. Stat. of the H. Comm. on Post Off. & Civ. Serv.*, 86th Cong. 17 (1959) [hereinafter *Census Plans Hearing*] (statement of Dr. Robert W. Burgess, Director, Bureau of the Census).

[39] *See Use of Electronic Data Processing: Hearing Before Subcomm. on Census & Gov't Stat. of the H. Comm. on Post Off. & Civ. Serv.*, 87th Cong. 142 (1962) [hereinafter *Electronic Data Processing: Hearing*] (statement of James F. Kelly, Deputy Administrative Assistant Secretary and Comptroller, Department of Health, Education, and Welfare).

[40] Act of Oct. 5, 1961, Pub. L. No. 87-397, sec. 6109, § 1(a), 75 Stat. 828 (1961) (current version at I.R.C. § 6109) (West).

[41] *See Electronic Data Processing: Hearing*, *supra* note 39, at 40 (statement of Glenn O. Stahl, Director, Bureau of Programs and Standards); *see also* STAFF OF H. SUBCOMM. ON CENSUS & GOV'T STAT. OF THE COMM. ON POST OFF. & CIV. SERV., 86TH CONG., REP. ON THE USE OF ELEC. DATA-PROCESSING EQUIP. IN THE FED. GOV'T 43 (Comm. Print 1960) [hereinafter DATA-PROCESSING REPORT].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

"national data bank" in the mid-1960s.[42] The 1970s also witnessed more expansion of welfare coverage and wider use of SSNs and technology.[43] During this period, the new technology and its capacity to process large numbers of files captured the imagination of high-level bureaucrats.

1. The Introduction of the Computer

The first large-scale data processing computer was delivered to the Bureau of the Census in April 1951 for its experimental use for the 1950 census.[44] A few years later, a second computer was purchased for the 1954 economic census.[45] By December 31, 1957, 121 electronic computers were installed throughout the federal government.[46] By June 30, 1960, the number jumped to 524, excluding those employed for classified use in the Department of Defense.[47] The Social Security Administration had its first computer installed in early 1956.[48] The Treasury Department, which had been interested in the technology since June 1953,[49] had its first computer installed in April 1958.[50] The number of computers continued to grow:

[42] STAFF OF S. COMM. ON GOV'T OPERATIONS & H. SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RTS. OF THE H. COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGIS. HIST. OF THE PRIV. ACT OF 1974 S. 3418 (PUB. L. 93-579) 298 (Joint Comm. Print 1976).

[43] *See infra* Section II.A.3.

[44] *Census Plans Hearing*, *supra* note 38. The computer, named UNIVAC (UNIVersal Automatic Computer), was produced by Electronic Control Company, a company established by John Presper Eckert and John W. Mauchly. *See* MARTIN CAMPBELL-KELLY, WILLIAM F. ASPRAY, JEFFREY R. YOST, HONHON TINN, GERARDO CON DIAZ & NATHAN ENSMENGER, COMPUTER: A HISTORY OF THE INFORMATION MACHINE 110 (2014). Eckert and Mauchly signed a contract with the Census Bureau in 1946. *Id.*

[45] *Census Plans Hearing*, *supra* note 38.

[46] *Use of Electronic Data Processing Equipment: Hearing Before the H. Subcomm. on Census & Gov't Stat. of the Comm. on Post Off. & Civ. Serv.*, 86th Cong. 4 (1959) (statements of Ellsworth H. Morse, Jr., Director, Acct. & Auditing Pol'y Staff, Gen. Acct. Off.; Edward J. Mahoney, Assistant Director, Acct. & Auditing Pol'y Staff, Gen. Acct. Off.); *see also id.* at 42–69.

[47] COM. GEN. OF THE U.S., COMPILATION OF GENERAL ACCOUNTING OFFICE FINDINGS AND RECOMMENDATIONS FOR IMPROVING GOVERNMENT OPERATIONS 89 (1962); DATA-PROCESSING REPORT, *supra* note 41, at 61.

[48] DATA-PROCESSING REPORT, *supra* note 41, at 40.

[49] *See id.* at 43.

[50] *Id.* at 51.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

by June 30, 1962, 1,006 computers were installed throughout the federal government.[51]

President John F. Kennedy, in his message to the House Ways and Means Committee on April 20, 1961,[52] noted that a system of identifying taxpayer account numbers "is an essential" part of his proposed improved collection and enforcement program, which would be adopting an "automatic data processing" technology.[53] Kennedy added, "[f]or this purpose, social security numbers would be used by taxpayers already having them."[54] Kennedy probably obtained advice from Mortimer M. Caplin, who had served on the President's Task Force on Taxation after Kennedy won the election in November 1960 and was appointed the IRS Commissioner in 1961.[55] Caplin saw the value of "automatic data processing" of federal tax returns and the connection with the SSN:

> To make ADP complete and workable, a positive identification device was needed. A numbering system was the obvious alternative. Ideal for this purpose was the social security number because of its almost universal usage by a substantial number of individual taxpayers.[56]

In October 1961, Congress amended the Internal Revenue Code, which allowed the Internal Revenue Service to use SSNs as identification numbers for filing tax

[51] BUREAU OF THE BUDGET, EXEC. OFF. OF THE PRESIDENT, INVENTORY OF AUTOMATIC DATA PROCESSING EQUIPMENT IN THE FEDERAL GOVERNMENT 13 (1962); *Electronic Data Processing: Hearing*, *supra* note 39, at 1 (statement of Rep. David N. Henderson, Chairman, Subcomm. on Census & Gov't Stat. of the H. Comm. on Post Off. & Civ. Serv.).

[52] JOHN F. KENNEDY, PRESIDENT'S TAX MESSAGE ALONG WITH PRINCIPAL STATEMENT, DETAILED EXPLANATION, AND SUPPORTING EXHIBITS AND DOCUMENTS 1 (1961), *in The President's Tax Recommendations: Hearings Before the H. Comm. on Ways & Means*, 87th Cong. 13 (1961) (written statement of President John F. Kennedy).

[53] *Id.* at 15.

[54] *Id.*; *see also id.* at 253–307.

[55] Eric Williamson, *Mortimer Caplin, Public Servant and UVA Law Professor Emeritus, Dies at 103*, UVATODAY (July 16, 2019), https://news.virginia.edu/content/mortimer-caplin-public-servant-and-uva-law-professor-emeritus-dies-103 [https://perma.cc/4XKE-WVJH].

[56] Mortimer M. Caplin, *The Taxpayer-Identifying Number System: The Key to Modern Tax Administration*, 49 A.B.A. J. 1161, 1162 (1963); *see also* Mortimer M. Caplin, *Automatic Data Processing of Federal Tax Returns*, PRAC. LAW. Oct. 1961, at 43.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

returns.[57] For the purpose of processing federal tax returns, a National Computer Center based in Martinsburg, West Virginia, equipped with an IBM computer system, was established in November of that year.[58] In 1962, the IRS started using the SSN as its taxpayer identification number.[59]

Use of the SSN was also shared with other departments: outgoing President Dwight D. Eisenhower issued Executive Order 10911 on January 17, 1961, which directed the IRS to make income tax returns "open to inspection by the Department of Commerce."[60] The Department of Treasury, through Treasury Decision 6547, issued an implementation of the Executive Order, providing that any such "information thus obtained shall be held confidential except that it may be published or disclosed in statistical form."[61] With this procedure, the United States Census Bureau could have access to the tax returns.[62] Cornelius E. Gallagher, a member of the House of Representatives, told the House Post Office and Civil Service Committee in August 1966:

> When coupled with social security numbers . . . such information could be made more readily available to any interested parties, be they benevolent or nonbenevolent. Evidently, it is the belief of the Bureau that the use of social security numbers would make it possible to combine census information with other already-collected data and still protect the confidentiality of the census information.[63]

Other federal agencies soon followed. In 1961, the U.S. Civil Service Commission began using the SSN as an identifying number for all federal employees

[57] Act of Oct. 5, 1961, Pub. L. No. 87-397, 75 Stat. 828 (codified as amended at 26 I.R.C. §§ 6109, 6676 (West)).

[58] IRS HIST. STUDS., IRS HISTORICAL FACT BOOK: A CHRONOLOGY 1646–1992, at 173–74 (1993).

[59] *Id.* at 176.

[60] Exec. Order No. 10911, 26 Fed. Reg. 509 (Jan. 20, 1961).

[61] T.D. 6547, 1961-1 C.B. 693.

[62] *Federal Government Paperwork (Part I): Hearings Before the Subcomm. on Census & Stat. of the H. Comm. on Post Off. & Civ. Serv.*, 89th Cong. 57–58 (1966) (statement of William H. Smith, Assistant Comm'r of Internal Revenue).

[63] *1970 Census Questions: Hearings Before the H. Comm. on Post Off. & Civ. Serv.*, 89th Cong. 3–4 (1966) (statement of Hon. Cornelius E. Gallagher, Rep. in Congress from New Jersey).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

for internal statistical purposes.[64] At this time, there were 2.4 million government workers.[65] John W. Macy, Jr., Chairman of the U.S. Civil Service Commission from 1961 to 1969, was both a visionary and zealous in recognizing the potential of computers in personnel management in the federal government.[66]

2. Proposals for a National Data Bank

With the introduction of the computer, there was a growing interest in establishing a centralized data center. In 1961, the Bureau of the Budget commissioned a feasibility study focused on the centralization and computerization of files and records held by individual agencies of the federal government.[67] The study was conducted by a group of scholars called the Committee on the Preservation and Use of Economic Data of the Social Science Research Council.[68] In April 1965, the Committee—chaired by Richard Ruggles, an economics professor at Yale University—issued a report recommending a "Federal Data Center" (the "Ruggles Report").[69] It recognized the impact of the computer on data processing as "a systematic evolution which has had far-reaching implications for the Federal statistics system ever since the original punchcard equipment was introduced."[70] The report asserted that a barrier to fully materializing the potential of the new technology was the "decentralized nature" of the federal statistical system.[71] Thus, the report recommended a centralized "Federal Data Center" established by the federal government, and that "[t]he first and most basic requirement of a Federal Data Center

[64] SOC. SEC. ADMIN., REPORT TO CONGRESS ON OPTIONS FOR ENHANCING THE SOCIAL SECURITY CARD (1991), https://www.ssa.gov/history/reports/ssnreportc2.html [https://perma.cc/A4XL-JHNQ].

[65] U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2003, at 94 (Supp. 2003).

[66] FRANK P. SHERWOOD, UNCOMMON PEOPLE I HAVE KNOWN: SIXTEEN INDIVIDUALS WHO HAVE MADE A DIFFERENCE 321 (2013). *See generally* John W. Macy, Jr., *Automated Government*, SATURDAY REV., July 1966, at 23.

[67] MEMBERS OF THE COMM. ON THE PRES. AND USE OF ECON. DATA, SOC. SCI. RSCH. COUNCIL, REPORT OF THE COMMITTEE ON THE PRESERVATION AND USE OF ECONOMIC DATA TO THE SOCIAL SCIENCE RESEARCH COUNCIL 3 (1965) [hereinafter THE RUGGLES REPORT]. For the context in which the Ruggles Report was developed, see Rebecca S. Kraus, *Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants*, 5 J. PRIV. & CONFIDENTIALITY, no. 1, 2013, at 1.

[68] *Report of Representatives to the Social Science Research Council*, AM. ECON. REV., May 1963, at 728, 729.

[69] THE RUGGLES REPORT, *supra* note 67, at 1.

[70] *Id.* at 8.

[71] *Id.* at 18.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

is that it should have the authority to obtain computer tapes produced by other Federal agencies."[72] The Ruggles Report also emphasized that a Federal Data Center would provide servicing facilities that would serve "somewhat the same role as the Library of Congress."[73]

The Ruggles proposal was quickly endorsed by two subsequent reports. The first was Dunn's report. Shortly after the Ruggles Report was received, the Bureau of the Budget employed Dr. Edgar S. Dunn, Jr. as a consultant to further study the feasibility of the Ruggles proposal.[74] A few months later, in November 1965, "Review of a Proposal for a National Data Center," better known as the Dunn Report, was transmitted to the Bureau of the Budget.[75] Dunn considered the Ruggles Report a "healthy beginning" in its evaluation of the problem and the recommendation of a national data center.[76] Dunn went further by emphasizing integration of files by improving file compatibility and accessibility,[77] and therefore the search functions of the proposed data center.[78] "Thus, the key . . . does not reside in the assembly of the records in a center but in the capacity to provide certain forms of file management and utilization service to the user."[79]

The third report was the Kaysen Report, prepared by the Task Force on the Storage of and Access to Government Statistics and chaired by Carl Kaysen, which

[72] *Id.* at 19.

[73] *Id.* at 20.

[74] Raymond T. Bowman, *Preface* to EDGAR S. DUNN, JR., REVIEW OF PROPOSAL FOR A NATIONAL DATA CENTER (1965) [hereinafter THE DUNN REPORT].

[75] *See generally* THE DUNN REPORT, *id.* According to Dunn, "This report . . . was prepared as an internal informal review and study document for the office of Statistical Standards of the Bureau of the Budget, upon the request of the Bureau of the Budget, because of a considerable amount of attention that was being brought to this issue." *Invasions of Privacy: Hearings Before the Subcomm. on Admin. Prac. and Proc. of the S. Comm. on the Judiciary*, 89th Cong. 2400 (1966) [hereinafter *Invasions of Privacy Hearings*] (statement of Dr. Edgar S. Dunn Jr., Research Associate, Resources for the Future, Inc.).

[76] THE DUNN REPORT, *supra* note 74, at 5.

[77] *See id.* at 16 ("In a fundamental way, file accessibility is the issue of file compatibility which is inseparable from the production practices that determine the organization and quality of the file.").

[78] *See id.* at 5 ("The greatest deficiency of the existing Federal Statistical System is its failure to provide access to data in a way that permits the association of the elements of data sets in order to identify and measure the interrelationship among interdependent activities.").

[79] *Id.* at 23.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

was submitted to the Bureau of the Budget in October 1966.[80] The Kaysen Report was prepared in the context of widespread privacy concerns about personal data, as well as a growing mistrust of the federal government in the era of the Vietnam War.[81] The Kaysen Report was clearly on the defensive, highlighting that the report's focus was on the federal *statistical* system.[82] Nevertheless, the Kaysen Report endorsed the idea of a "National Data Center" responsible for "assembling in a single facility all large-scale systematic bodies of demographic, economic, and social data generated by the present data-collection or administrative processes of the Federal Government."[83] Kaysen explained in March 1967 that the reason his committee used "National Data Center" instead of "Federal Data Center" was that they wanted state and local information put in the data center.[84] Kaysen also described the key function of SSNs in the proposed "National Data Center":

> For the data center to achieve its intended purposes, the material in it must identify individual respondents in some way, by social security number, for individuals . . . . Without such identification, the center cannot meet its prime purpose of integrating the data collected by various agencies into a single consistent body.[85]

The proposals for a centralized data center immediately caused a public outcry after the Ruggles Report was made public.[86] In June 1966, the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary

[80] CARL KAYSEN, CHARLES C. HOLT, RICHARD HOLTON, GEORGE KOZMETSKY, H. RUSSELL MORRISON & RICHARD RUGGLES, REPORT OF THE TASK FORCE ON THE STORAGE OF AND ACCESS TO GOVERNMENT STATISTICS (1966) [hereinafter THE KAYSEN REPORT].

[81] PEW RESEARCH CENTER, BEYOND DISTRUST: HOW AMERICANS VIEW THEIR GOVERNMENT 18 (2015), https://www.pewresearch.org/politics/2015/11/23/1-trust-in-government-1958-2015/ [https://perma.cc/K7U8-C2HU].

[82] THE KAYSEN REPORT, *supra* note 80, at 2.

[83] *Id.* at 17.

[84] *Computer Privacy: Hearings Before the Subcomm. on Admin. Prac. and Proc. of the Comm. on the Judiciary*, 90th Cong. 31 (1967) (statement of Carl Kaysen, Director, Institute for Advanced Study, Princeton University).

[85] *Id.* at 4–5.

[86] Kraus, *supra* note 67, at 1.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

invited Dunn to testify on the proposals.[87] Dunn largely dismissed personal privacy concerns.[88] In July 1966, the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations ("House Special Subcommittee") invited Raymond T. Bowman, then Assistant Director for Statistical Standards, Bureau of the Budget, to testify.[89] Bowman clarified that they were setting up a "Federal *Statistical* Data Center."[90] More specifically, Bowman told the House Special Subcommittee:

> The Dunn report and the Ruggles report . . . were just not careful enough in their wording. What they were thinking about and at least what we were interested in, in reviewing their proposals, was not a data center for all purposes, but a Federal Statistical Data Center.[91]

Bowman repeatedly assured the House Special Subcommittee that there was "no intention to organize the data in the center with regard to individuals."[92] In doing so, Bowman had either deliberately downplayed the central point of the National Data Center proposals or wholeheartedly embraced computer technology with no concern for the danger associated with it. John W. Macy, Jr. showed a similar perspective in an article published in the *Saturday Review* in July 1966, shortly before Bowman's testimony.[93] In this article, Macy urged that in the computer age "we must have integrated information systems. This will require the use of information across

---

[87] *Invasions of Privacy Hearings*, *supra* note 75, at 2389.

[88] *Id.* at 2390.

> I would claim that the sets of data under the intent of this proposal are at the end of the spectrum for the personal privacy issue conflicts least with public interest. They do not contain sensitive personal intelligence. They are more characteristically demographic and economic data, identifying attributes such as age, sex, and occupational characteristics that are more commonly associated with the public face of the individual.

Id.

[89] *See The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the H. Comm. on Gov't Operations*, 89th Cong. 49 (1966) (statement of Raymond T. Bowman, Assistant Director for Statistical Standards, Bureau of the Budget).

[90] *Id.*

[91] *Id.* at 53.

[92] *Id.*

[93] Macy, *supra* note 66.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

departmental boundaries."[94] Macy did not refer to the "National Data Center" in his article, but he clearly shared the vision.[95]

3. Welfare Expansion in 1972

In the 1970s, the federal government further pushed for a centralized data system. Senator Sam J. Ervin Jr. remarked in March 1971, at a Senate hearing, "[t]he increasing use of [the SSN] to identify the individual has made it one of the prime symbols of the computer age."[96] He noted that an SSN was constantly required in Department of Health, Education and Welfare questionnaires, "voter registration affidavits; telephone company records; nursing registration forms; credit applications, arrest records; military records; drivers licenses; death certificates; and insurance records."[97]

On May 12, 1971, a Social Security Task Force report further confirmed the trend toward using the SSN as the universal identification number: "We think it is clear from this by-no-means exhaustive survey that the SSN is already well established as a multipurpose identifier in all sectors of society."[98] Framing this historic moment as "the SSN at the crossroads," the Task Force stated unequivocally that "we believe the Nation stands to gain a great deal from a fuller exploitation of the SSN as a mechanism for the efficient and economical collection and exchange of personal data."[99] Furthermore, the Task Force believed that "the wider use of the SSN would be particularly beneficial in such areas as health, education, and welfare—areas in which resources are limited and the need for more efficient operations is great."[100]

---

[94] *Id.* at 25.

[95] *See* Macy, *supra* note 66.

[96] *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary*, 92d Cong. 776 (1971) [hereinafter *Federal Data Banks Hearings*].

[97] *Id.*

[98] SOC. SEC. NO. TASK FORCE, REPORT TO THE COMMISSIONER, SOCIAL SECURITY ADMINISTRATION, DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE (1971), *in Privacy: The Use, Collection, and Computerization of Data: J. Hearings Before the Ad Hoc Subcomm. on Priv. & Info. Sys. of the Comm. on Gov't Operations*, 93d Cong. 1167 (1971). The Social Security Number Task Force was formed on March 30, 1970, by Commissioner of Social Security, Robert M. Ball. *Id.* at 1160.

[99] *Id.* at 1172.

[100] *Id.* at 1173.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In October 1972, the Social Security Act was amended to allow any individual applying for federally funded benefits to have an SSN.[101] In May 1971, when the amendments were in deliberation in Congress, the House Committee on Ways and Means noted that the use of false names and SSNs "has led to a number of problems in both private business and the administration of Government programs."[102] Thus, the Committee proposed to create penalties for giving false information in order to obtain an SSN.[103] The proposal was well received and found its way into the new law.[104] Believing that it had fixed the problem, the Committee suggested that the SSN should be used "to identify every recipient."[105] According to the House Committee,

> [t]he use of the social security number will also permit the information concerning a family's earnings and other income to be checked against the Social Security Administration's earnings and benefit files, as well as the files of the Railroad Retirement Board, Veterans Administration, Internal Revenue Service, Civil Service Commission, and State employment service. It is expected that subsequent regular periodic checks against these data files will be made.[106]

Clearly, the House Committee expected federal agencies to share data with each other in their fight against abuse of the welfare system. But the House Committee was not alone. In the testimony from Ronald Reagan, then California Governor, and Robert B. Carleson, Director of Social Welfare in California,[107] Reagan argued in favor of letting the states manage social welfare programs because, according to Reagan, "States are better equipped than the Federal Government to administer effective welfare reforms."[108] According to Carleson:

---

[101] Act of Oct. 30, 1972, Pub. L. No. 92-603, 86 Stat. 1329 (codified as amended at 42 U.S.C. § 405).

[102] H.R. REP. NO. 92-231, at 64 (1971).

[103] *Id.*

[104] *See* 42 U.S.C. § 408.

[105] H.R. REP. NO. 92-231, at 188 (1971).

[106] *Id.* at 189.

[107] *Social Security Amendments of 1971: Hearings on H.R. 1 Before the S. Comm. on Finance*, 92d Cong. 1873 (1972) (statement of Hon. Ronald Reagan, Governor of the State of California).

[108] *Id.* at 1874.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

> We have . . . developed a statewide data processing system which we are not long from implementing which will permit us to cross check between counties and even though the counties would still be administering welfare at the local level, we get the advantage of statewide cross checking.[109]

Then Senator Jack Miller (Iowa) asked if this was done by using the SSN.[110] Carleson replied:

> Yes, Senator, limiting people to one number, for instance, permitting access to the information in the social security system and also in the Internal Revenue System and other similar systems.
>
> Our new California program will permit this now within our own State system, in other words, our own employment security system, our State income tax system and otherwise, and to be able to expand this into the Federal system would be of great benefit.[111]

As a result, the Social Security Act of 1972 greatly expanded coverage of social welfare—it extended to 10 million persons eligible for Aid to Families with Dependent Children ("AFDC").[112]

B. The SSN in the Federal Courts Before the Privacy Act

Before the Privacy Act of 1974, federal agencies widely exercised power demanding SSNs in their investigative processes via a tool called "administrative summons" served on third-party defendants. The Supreme Court, through the "third-party doctrine," maintained a very deferential position, unwilling to provide a check on the power of the federal agencies.[113]

---

[109] *Id.* at 1890.

[110] *Id.*

[111] *Id.*

[112] H.R. REP. NO. 92-231, at 2 (1971).

[113] *See, e.g.*, United States v. Miller, 425 U.S. 435, 444 (1976); California Bankers Ass'n v. Shultz, 416 U.S. 21, 51–53 (1974); Joseph R. Mangan, Jr., *Reasonable Expectations of Privacy in Bank Records: A Reappraisal of* United States v. Miller *and Bank Depositor Privacy Rights*, 72 J. CRIM. L. & CRIMINOLOGY 243, 244–45 (1981); Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1294–95 (1981); Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 260–61 (1984); Dean Galaro, *A Reconsideration of Financial Privacy and* United States v. Miller, 59 S. TEX. L. REV. 31, 33–34 (2017). For defense of the third-party doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Donaldson v. United States involved an investigation on Kevin L. Donaldson in September 1968, where Internal Revenue Service agents served summonses on Donaldson's former employer, Acme Circus Operating Co., Inc., and the latter's accountant, Joseph J. Mercurio, ordering them to produce Acme's records of Donaldson, including his social security number.[114] In November 1968, the IRS filed a petition in a federal district court seeking enforcement of the summonses under 26 U.S.C. Sections 7402(b) and 7604(a).[115] In response to the enforcement proceedings, Donaldson filed a motion to intervene.[116] The district court denied Donaldson's motion and directed the employer to comply with summons.[117] The Fifth Circuit affirmed.[118]

At the time, federal circuit courts were split on the question of whether a taxpayer could intervene in proceedings involving a request for their record from a third party. The Fifth Circuit, joining the First and Second Circuits, was of the opinion that a taxpayer was not entitled to intervene.[119] For these circuits, the fact that records sought by the IRS were property of a third party, not that of the taxpayer, was an essential factual element that had significant legal consequences.[120] This

---

MICH. L. REV. 561 (2009), and Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2009).

[114] 400 U.S. 517, 518–19 (1971). *See* Michael Hatfield, *Privacy in Taxation*, 44 FLA. ST. U. L. REV. 579, 597 (2017) ("The IRS collects information from [both] taxpayers and third parties. Taxpayers are obligated to maintain adequate records, making them available to the IRS. Third parties report information on 97% of taxpayers.").

[115] *Donaldson*, 400 U.S. at 520.

[116] *Id.* at 521.

[117] *Id.* at 521–22.

[118] United States v. Mercurio, 418 F.2d 1213, 1218 (5th Cir. 1969).

[119] *Id.*; *In re* Cole, 342 F.2d 5, 7 (2d Cir. 1965) (holding that IRS was not required to give notice to taxpayers when their bank was summoned to produce records relating to them); O'Donnell v. Sullivan, 364 F.2d 43, 44 (1st Cir. 1966) (holding that taxpayer had no standing to intervene when his bank was summoned to produce records relating to him).

[120] *Mercurio*, 418 F.2d at 1214.

> It may clarify the discussion here to begin by stating what is *not* involved. We do *not* have a case in which a subpoena has been issued at the instance of a special agent of the Internal Revenue Service against a *taxpayer* himself, seeking access to his records and papers and the right to take his testimony . . . nor is it a case in which the subpoena seeks to obtain records of *the taxpayer* in the hands of his attorney or accountant, which the courts have deemed the same as if they were in the possession of the taxpayer himself.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

characterization of the requests for information avoided constitutional issues—such as unreasonable searches and seizures under the Fourth Amendment and the self-incrimination privilege under the Fifth Amendment.[121]

The other circuits included the Seventh, Third, and Sixth, which were of the opinion that a taxpayer is entitled to intervention.[122] For these courts, the fact that records sought by the IRS were not the taxpayer's property was not the end of the inquiry; it was not even a significant factor. Citing the Supreme Court's earlier

---

Id. (emphasis added). *In re* Cole, 342 F.2d at 7–8.

> The distinguishing feature of the present case is that all of the records, documents and papers which were the subject matter of the summons were the property of the Bank on whom the summons was served. None of the material sought belonged to the taxpayers or involved the work product of their attorneys. They had no interest in any of them in the sense that they had a right to any of them. Under these circumstances the Commissioner had no duty to give advance notice to the taxpayers or their counsel of his intention to examine a third party and the third party's own records and papers.

Id. Sullivan, 364 F.2d at 44.

> Appellant cannot claim these records, kept by the bank for its own purposes, as his property. Nor can he invoke the attorney-client privilege. These were not confidential communications to an attorney by a client. They had already been disclosed to a third party, the bank. They were not the property of a client.

Id.

[121] *See* U.S. CONST. amend. IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.; *see also id.* amend. V. ("No person . . . shall be compelled in any criminal case to be a witness against himself . . . .").

[122] *See, e.g.*, United States v. Benford, 406 F.2d 1192, 1194 (7th Cir. 1969) ("We interpret them as adopting the judicial policy with respect to I.R.S. inquisitorial summonses that the person whose tax liability is the subject of the investigation can intervene and challenge enforcement if he sees fit."); United States v. Bank of Com., 405 F.2d 931, 935 (3d Cir. 1969) ("Accordingly, we hold that the district court should hear and determine appellant's Fourth Amendment claim and thus assure itself that its process will not be abused."); Justice v. United States, 365 F.2d 312, 314 (6th Cir. 1966) ("This Court is of the opinion that unless the Taxpayers are permitted to intervene, they would not be aggrieved parties, entitling them to an appeal."); *see also* Louis L. Jaffe, *The Judicial Enforcement of Administrative Orders*, 76 HARV. L. REV. 865 (1963).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

decisions in *Reisman v. Caplin* and *United States v. Powell*,[123] these courts reasoned that trial courts needed to examine the nature of the taxpayer's interest in protecting the records sought by the IRS to assess the constitutional and statutory issues.[124]

The *Donaldson* Court sided with the Fifth Circuit. Affirming the latter's decision, the Court wholly endorsed the Fifth Circuit's position, stating that "there is now no constitutional issue in the case."[125] Here, the Supreme Court embraced the third-party property framework underlying the Fifth Circuit's decision. Like the Fifth Circuit, the *Donaldson* Court highlighted: "We emphasize initially . . . that what is sought here by the Internal Revenue Service from Mercurio and from Acme is the production of *Acme*'s records and not the records of the *taxpayer*."[126] And that:

> Each of the summonses here, we repeat, was directed to a third person with respect to whom no established legal privilege, such as that of attorney and client, exists, and had to do with records in which the taxpayer has no proprietary interest of any kind, which are owned by the third person, which are in his hands, and which relate to the third person's business transactions with the taxpayer.[127]

This way, constitutional issues were kept out of the picture. The rest of the *Donaldson* reasoning was based on two issues: The first one was Section 7602 of the Internal Revenue Code, which enables the IRS to summon any person having

---

[123] *See* Reisman v. Caplin, 375 U.S. 440 (1964); United States v. Powell, 379 U.S. 48 (1964).

[124] *Benford*, 406 F.2d at 1194.

> Thus, in both *Reisman* and *Powell*, the taxpayers could spell out such relationship with the records sought that compulsion of disclosure might arguably impair taxpayers' constitutional or other legally protected rights. In each case, the taxpayer's basis for intervention was a demonstrated 'interest' more specific and palpable than his concern that the evidence might aid the government in increasing his liability for taxes.

Id.; *Bank of Commerce*, 405 F.2d at 935 ("It is clear that the appellant's contention would be entitled to consideration were he alleging that enforcement of the summonses would constitute an unreasonable search and seizure in violation of his Fourth Amendment rights, assuming the requisite standing."); *Justice*, 365 F.2d at 314 ("The [Supreme] Court [in *Reisman* and *Powell*] finds it is probable that the representation of the Taxpayers' interest by existing parties may be inadequate, and that the Taxpayers may be bound by a judgment in the action.").

[125] Donaldson v. United States, 400 U.S. 517, 522 (1971).

[126] *Id.* at 522–23 (emphasis added).

[127] *Id.* at 523.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

possession of books, papers, or records that may be relevant or material to a tax investigation.[128] On this issue, the *Donaldson* Court gave a broad interpretation by concluding that even if an IRS summons under Section 7602 led to criminal prosecution of the taxpayer, the statute would allow the IRS summons to be "issued in aid of an investigation if it is issued in good faith and prior to a recommendation for criminal prosecution."[129] The second issue the Court dealt with was Rule 24(a)(2) of Federal Rules of Civil Procedure, which regulates intervention.[130]

[128] *Id.* at 524–25. Section 7602 of the Internal Revenue Code provides that:

> For the purpose of ascertaining the correctness of any return, making a return where none has been made, determining the liability of any person for any internal revenue tax or the liability at law or in equity of any transferee or fiduciary of any person in respect of any internal revenue tax, or collecting any such liability, the Secretary is authorized—
> (1) To examine any books, papers, records, or other data which may be relevant or material to such inquiry;
> (2) To summon the person liable for tax or required to perform the act, or any officer or employee of such person, or any person having possession, custody, or care of books of account containing entries relating to the business of the person liable for tax or required to perform the act, or any other person the Secretary may deem proper, to appear before the Secretary at a time and place named in the summons and to produce such books, papers, records, or other data, and to give such testimony, under oath, as may be relevant or material to such inquiry; and
> (3) To take such testimony of the person concerned, under oath, as may be relevant or material to such inquiry.

I.R.C. § 7602(a).

[129] *Donaldson*, 400 U.S. at 536.

[130] *Id.* at 527–28. Rule 24(a) of the Federal Rules of Civil Procedure provides, in relevant part:

> On timely motion, the court must permit anyone to intervene who . . .
> (2) claims an interest relating to the property or transaction that is the subject of the action, and is so situated that disposing of the action may as a practical matter impair or impede the movant's ability to protect its interest, unless existing parties adequately represent that interest.

FED. R. CIV. P. 24(a). The *Donaldson* Court found that a third party in a summary enforcement proceeding may intervene with permission from a district court, but the third party may not intervene as an absolute right. *Donaldson*, 400 U.S. at 529.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In sum, *Donaldson* expanded the powers of the IRS in obtaining SSNs in its administrative processes. *Donaldson* was followed by a series of Supreme Court rulings in the 1970s in the direction of expanding the powers of the IRS.[131]

II. THE PRIVACY REVOLUTION

The notion of a constitutional right to privacy started with Samuel Warren and Louis Brandeis' 1890 article in *Harvard Law Review*.[132] In subsequent years, however, judicial recognition of privacy was slow and tenuous. At the center of the debate was whether privacy should be understood as based on property interests. For Warren and Brandeis, the essence of the right to privacy was "not the principle of private property, but that of an inviolate personality."[133] Roscoe Pound and his associates shared the same view.[134] The Supreme Court adopted the property-centered position in 1928 in *Olmstead v. United States*.[135] There, the Court ruled that the police's wiretapping of a telephone line of the defendant was not a "search" under the Fourth Amendment because there was no trespass to the defendant's property.[136]

---

[131] *See, e.g.*, Couch v. United States, 409 U.S. 322 (1973) (holding that a taxpayer may not invoke their Fifth Amendment privilege against compulsory self-incrimination to prevent the production of her business and tax records in the possession of her accountant); United States v. Bisceglia, 420 U.S. 141 (1975) (holding that the IRS has statutory authority to issue a "John Doe" summons to a bank or other depository to discover the identity of a person who has had bank transactions suggesting the possibility of liability for unpaid taxes); United States v. LaSalle Nat'l Bank, 437 U.S. 298 (1978) (clarifying the limits of the good-faith use of an Internal Revenue summons issued under section 7602).

[132] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[133] *Id.* at 205; see *id.* at 211 ("The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested."); *see also* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962, 971 (1964) (arguing that "inviolate personality" is the "most significant indication of the interest [Warren and Brandeis] sought to protect" by the notion of a right to privacy).

[134] *See* Roscoe Pound, *Equitable Relief Against Defamation and Injuries to Personality*, 29 HARV. L. REV. 640 (1916); Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343 (1915). Other works following this line of advocacy include Wilbur Larremore, *Law of Privacy*, 12 COLUM. L. REV. 694 (1912); Zechariah Chafee, Jr., *Progress of the Law 1919–1920*, 34 HARV. L. REV. 388, 407–14 (1921); Joseph R. Long, *Equitable Jurisdiction to Protect Personal Rights*, 33 YALE L.J. 115, 122–26 (1923) (discussing the right to privacy); and Leon Green, *Right of Privacy*, 7 U. ILL. L. REV. 237 (1932).

[135] 277 U.S. 438 (1928).

[136] *Id.* at 464 ("The [Fourth A]mendment itself shows that the search is to be of material things-the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or *things* to be seized.") (emphasis added).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Brandeis, then sitting on the bench as Associate Justice, wrote the famous dissenting opinion.[137]

By the 1960s, Brandeis's dissenting opinion was gaining broader support. In 1967, the Supreme Court substantially reversed *Olmstead* in *Katz v. United States*.[138] But the ruling in *Donaldson* seemed to suggest that the Court switched back to the property theory.[139] This made it even more imperative for Congress to act. New technology, from eavesdropping devices to the recently introduced computer, added urgency to call for a new notion of privacy. Congress intended to respond to these concerns quickly with the Freedom of Information Act in 1967,[140] the Fair Credit Reporting Act in 1970,[141] and the Privacy Act in 1974.[142]

A. Actors and Leaders

Shortly before the introduction of the computer, privacy had already gained attention from a variety of connected sources: first, George Orwell's novel *1984* was published in 1949, which became popular on both sides of the Atlantic.[143] Second, eavesdropping gadgets became cheap and widely available in the 1950s, making the practice of wiretapping and eavesdropping more widespread.[144] Third, many Americans had their exposure to surveillance during the McCarthy Era of the

[137] *Id.* at 471–85 (Brandeis, J., dissenting).

[138] 389 U.S. 347, 353 (1967). Two years before the *Katz* decision, the Supreme Court recognized privacy rights in *Griswold v. Connecticut*, 381 U.S. 479, 483–84 (1965).

[139] *See Donaldson*, 400 U.S. at 536.

[140] Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552).

[141] Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1830-1831 and 15 U.S.C. § 1681 *et seq.*).

[142] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[143] *See* John Sutherland, *How '1984' Became an Overnight Sensation*, DAILY BEAST (Dec. 18, 2017, 8:39 PM), https://www.thedailybeast.com/how-1984-became-an-overnight-sensation [https://perma.cc/JS85-HU28].

[144] *See* Brian Hochman, *Eavesdropping in the Age of* The Eavesdroppers*; or, The Bug in the Martini Olive*, POST45 (Feb. 3, 2016), https://post45.org/2016/02/eavesdropping-in-the-age-of-the-eavesdroppers-or-the-bug-in-the-martini-olive/ [https://perma.cc/WZE7-LHMQ].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

1950s.[145] Therefore, the battle for privacy had to start from correcting the wrong of *Olmstead*.

Alan F. Westin, a young lawyer and scholar who graduated from Harvard Law School in 1951, became interested in civil liberty issues including wiretapping.[146] Westin's article, published in 1952, argued in favor of a federal law regulating wiretapping.[147] The American Civil Liberties Union ("ACLU") was opposed to wiretapping in general; however, if Congress would permit it, safeguards should be in place to protect the public's privacy interests.[148] The best-known critic of wiretapping in the 1950s was Samuel Dash, the district attorney in Philadelphia, Pennsylvania, from 1955 to 1956.[149] In the summer of 1956, Dash was recruited by the Pennsylvania Bar Association to conduct a detailed study on the practice of wiretapping across the United States.[150] The Dash Report brought the concerns of privacy to broader audience.[151]

---

[145] *See* Christopher M. Elias, *How McCarthyism, the Rise of Tabloids, and J. Edgar Hoover's Quest to Prove Himself "Manly" Led to a Surveillance State*, CRIMEREADS (May 28, 2021), https://crimereads.com/mccarthy-hoover-surveillance/ [https://perma.cc/8TNS-5MU6].

[146] *See, e.g.*, Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165 (1952) [hereinafter Westin, *Wire-Tapping Problem*]; Alan F. Westin, *Book Review*, 52 COLUM. L. REV. 948 (1952) (reviewing THE STATES AND SUBVERSION (Walter Gellhorn ed., 1952)); Alan F. Westin, *Book Review*, 61 YALE L.J. 451, 458 (1952) (reviewing HENRY STEELE COMMAGER, ROBERT K. CARR, ZECHARIAH CHAFEE JR., WALTER GELLHORN, CURTIS BOK & JAMES P. BAXTER III, CIVIL LIBERTIES UNDER ATTACK (1951)); ALAN F. WESTIN, THE CONSTITUTION AND LOYALTY PROGRAMS: PUBLIC EMPLOYMENT AND GOVERNMENTAL SECURITY (1954); Richard C. Donnelly, *Comments and Caveats on the Wire Tapping Controversy*, 63 YALE L.J. 799 (1954).

[147] Westin, *Wire-Tapping Problem*, *supra* note 146, at 165.

[148] *See* Mickie Edwardson, *James Lawrence Fly, the FBI, and Wiretapping*, 61 HISTORIAN 361, 378–79 (1999). A similar testimony was given by Mr. Irving Ferman, Director of the ACLU's Washington, DC Office. *See Wiretapping for National Security: Hearings on H.R. 408, H.R. 477, H.R. 3552, and H.R. 5149 Before Subcomm. No.3 of the H. Comm. on the Judiciary*, 83d Cong. 60 (1953) (statement of Irving Ferman, Director of the American Civil Liberties Union).

[149] *See* Warren E. Leary, *Samuel Dash, Chief Counsel for Senate Watergate Committee, Dies at 79*, N.Y. TIMES (May 30, 2004), https://www.nytimes.com/2004/05/30/us/samuel-dash-chief-counsel-for-senate-watergate-committee-dies-at-79.html [https://perma.cc/N79N-XYJA].

[150] SAMUEL DASH, RICHARD F. SCHWARTZ & ROBERT E. KNOWLTON, THE EAVESDROPPERS (1959). The study was sponsored by the Pennsylvania Bar Association Endowment under a grant from the Fund for the Republic. *Id.* at 5.

[151] A symposium was held at the University of Minnesota shortly after the publication of Dash's report. *See* Symposium, *The Wiretapping-Eavesdropping Problem: Reflections on* The Eavesdroppers, 44 MINN. L. REV. 813 (1960); Steven H. Goldblatt, *Remarks at the Georgetown University Law Center Memorial Service for Samuel Dash*, 42 AM. CRIM. L. REV. 5 (2005).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In 1958 and 1959, the Subcommittee on Constitutional Rights of the U.S. Senate Committee on the Judiciary, chaired by Senator Olin D. Johnston (D-SC), launched a series of hearings on wiretapping and eavesdropping, and both Westin and Dash were invited to give testimony.[152] In May 1961, the Constitutional Rights Subcommittee, now chaired by Senator Sam J. Ervin, Jr. (D-NC), initiated another series of hearings in consideration of legislative bills on wiretapping.[153] Senator Edward V. Long, the Missouri Democrat who served in the U.S. Senate from 1960 until 1968, chaired the Senate Subcommittee on Administrative Practice and Procedure in 1964.[154] In that capacity, Senator Long led the investigation on wiretapping and eavesdropping surveillance activities by federal law enforcement agencies through a series of hearings from 1965 to 1966.[155]

Cornelius E. Gallagher, member of the House from New Jersey's thirteenth congressional district from 1959 until 1973, played a crucial role.[156] In April 1963, Representative Gallagher proposed a study which resulted in congressional investigation of polygraphs.[157] From June 1965 to May 1966, Representative Gallagher led a Special Inquiry on Invasion of Privacy by a Subcommittee in the House Committee on Government Operations regarding the federal government's investigative and data-gathering activities.[158]

---

[152] *Wiretapping, Eavesdropping, and the Bill of Rights: Hearing Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary*, 85th Cong. 194 (1958) (statement of Prof. Alan Westin, Department of Government, Cornell University); *Wiretapping, Eavesdropping, and the Bill of Rights: Hearing Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary*, 86th Cong. 503 (1959) (statement of Samuel Dash).

[153] *Wiretapping and Eavesdropping Legislation: Hearings on S. 1086, S. 1221, S. 1495, and S. 1822 Before the Subcomm. on Const. Rts. of the Comm. on the Judiciary*, 87th Cong. 1 (1961).

[154] *Edward V. Long (1908–1972)*, MO. ENCYC. (July 22, 2022), https://missouriencyclopedia.org/people/long-edward-v [https://perma.cc/65HB-DUHP].

[155] *Invasions of Privacy (Government Agencies): Hearings Before the Subcomm. on Admin. Prac. and Proc. of the S. Comm. on the Judiciary*, 89th Cong. (1965). Senator Long also published a book of his own during this period of time. *See* EDWARD V. LONG, THE INTRUDERS: THE INVASION OF PRIVACY BY GOVERNMENT AND INDUSTRY (1966). For comments on Senator Long's book, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 119 (1995).

[156] *See* H.R. REP. NO. 89-198, at 5, 43 (1965).

[157] *See id.* at 1.

[158] *See Special Inquiry on Invasion of Privacy: Hearing Before a Subcomm. of the H. Comm. on Gov't Operations*, 89th Cong. 1 (1966).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

The most consequential advocate for privacy in the U.S. Senate was Senator Ervin, who served from 1954 to 1974.[159] As mentioned earlier, Senator Ervin chaired the Subcommittee on Constitutional Rights starting in 1961, and, in 1967, Ervin became increasingly concerned about computer use and abuse of its power.[160] Eventually, it was through Senator Ervin's persistence that the Privacy Act of 1974 was passed.[161]

Vance Packard, author of *The Naked Society*, was invited to testify in House hearings in 1966.[162] By the mid-1960s, George Orwell had been fully embraced in American intellectual life: "Now his reputation was firmly established, his books sold well, and he was constantly quoted."[163] Other authors embraced the topic, including Martin L. Gross with *The Brain Watchers*,[164] Myron Brenton with *The Privacy Invaders*,[165] and Jerry M. Rosenberg with *The Death of Privacy*.[166] The law

[159] *See* SAM JAMES ERVIN, JR., PRESERVING THE CONSTITUTION: THE AUTOBIOGRAPHY OF SENATOR SAM J. ERVIN, JR. 71–91 (1984). *See generally* KARL E. CAMPBELL, SENATOR SAM ERVIN, LAST OF THE FOUNDING FATHERS (2007).

[160] *The Computer and Individual Privacy*, 113 CONG. REC. 5898 (1967) (statement of Sen. Sam J. Ervin, Jr.); *The Computer and Individual Privacy*, 115 CONG. REC. 33576 (1969); *Secret Service Guidelines: Protection of the President and Protection of Individual Rights*, 115 CONG. REC. 39114 (1969) (statement of Sen. Sam J. Ervin, Jr.); Sam J. Ervin, Jr., *Privacy and Government Investigations*, 1971 U. ILL. L.F. 137 (1971).

[161] *Overview of the Privacy Act: 2020 Edition*, U.S. DEP'T OF JUST. (Oct. 4, 2022), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction [https://perma.cc/ZCV9-SQLK].

[162] Margaret O'Mara, *The End of Privacy Began in the 1960s*, N.Y. TIMES (Dec. 5, 2018), https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html [https://perma.cc/6B4L-6R3N]; *see also The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the H. Comm. on Gov't Operations*, 89th Cong. 7 (1966) [hereinafter *Computer and Invasion of Privacy Hearings*] (statement of Vance Packard, sociologist, author, and lecturer).

[163] John P. Rossi, *America's View of George Orwell*, 43 REV. POL. 572, 580 (1981).

[164] *Martin L. Gross*, HARPERCOLLINS PUBLISHERS, https://www.harpercollins.com/blogs/authors/martin-l-gross-880000020285 [https://perma.cc/D589-7YY7] (last visited Sept. 2, 2024).

[165] *Books by Myron Brenton*, GOODREADS, https://www.goodreads.com/author/list/937207.Myron_Brenton [https://perma.cc/M9XJ-28GN] (last visited Sept. 2, 2024).

[166] *The Death of Privacy*, KIRKUS REVS., https://www.kirkusreviews.com/book-reviews/a/jerry-m-rosenberg/the-death-of-privacy/ [https://perma.cc/6CY5-GE5Z] (last visited Sept. 2, 2024).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

journal *Law and Contemporary Problems* held a symposium on privacy in the spring of 1966, including authors like William M. Beaney and Edward Shils.[167]

B. Against the Federal Data Bank

The debate over the federal data bank was conducted in a series of congressional hearings: The first hearing was titled "The Computer and the Invasion of Privacy," by a Special Subcommittee on Invasion of Privacy under the House Committee on Government Operations in July 1966.[168] The second hearing was titled "Computer Privacy" by the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary from March 1967 to February 1968.[169] The third hearing was titled "Federal Data Banks, Computers, and the Bill of Rights," by the Subcommittee on Constitutional Rights of the Committee on the Judiciary in February 1971.[170]

1. The House Hearing in July 1966

The House hearing on "The Computer and Invasion of Privacy" happened in July 1966, right in the middle of the federal data bank controversy; it was after the Ruggles Report was published in April 1965 but before the Kaysen Report was completed in October 1966.[171] On the supporting side, Congressman Gallagher invited Ruggles, Dunn, and Bowman to the hearing.[172] On the opposing side, two prominent critics were invited: Vance Packard, a journalist and author,[173] and Charles A. Reich,[174] a law professor from Yale.

---

[167] *See* Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 L. & CONTEMP. PROBS. 281 (1966); William M. Beaney, *The Right to Privacy and American Law*, 31 L. & CONTEMP. PROBS. 253, 253 n.4 (1966).

[168] *Computer and Invasion of Privacy Hearings*, *supra* note 162, at 1.

[169] *Computer Privacy: Hearings before the Subcomm. on Admin. Prac. & Proc. of the S. Comm. on the Judiciary*, 90th Cong. (1967) [hereinafter *Computer Privacy Hearings*] (chaired by Senator Edward V. Long).

[170] *See Federal Data Banks Hearings*, *supra* note 96.

[171] *See* Steven Ruggles & Diana L. Magnuson, *"It's None of Their Damn Business": Privacy and Disclosure Control in the U.S. Census, 1790–2020*, 49 POPULATION & DEV. REV. 651, 663 (2023); *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 402 (1968) (discussing the Kaysen Report).

[172] *See Computer and Invasion of Privacy Hearings*, *supra* note 162, at iii.

[173] *Id.* at 7 (statement of Vance Packard).

[174] *Id.* at 22 (statement of Charles A. Reich, Professor, Yale Law School).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Vance Packard was the prominent author of the popular book *The Naked Society*.[175] It was Packard's book that partially prompted the House to start the hearings on national data bank proposals.[176] At the House hearing, Packard expressed his skepticism of the promises made by proponents of the data bank. He told the House Subcommittee that "[w]e should be wary of promises that the goals of such consolidation of data are only modest ones that would interest statisticians and planners. Unless there are safeguards, pressures will surely grow to assemble more and more specific data about specific individuals."[177] Packard linked the wide-range reckless data gathering with George Orwell's *1984*, and commented that "Big Brother, if he ever comes to the United States, may turn out to be . . . a relentless bureaucrat obsessed with efficiency."[178] Packard probably captured the central theme of the House hearings when he warned, "[i]n all these plans for centralizing data about citizens it seems to me that the crucial question is whether we are letting technology get out of hand without being sufficiently concerned about human values."[179]

Charles A. Reich was a prominent constitutional scholar in the 1960s.[180] His interest in privacy was prompted by the midnight searches conducted by welfare agencies to verify welfare recipients' honesty about their conditions.[181] Reich argued that in a welfare state, "a new zone of privacy" must be drawn in order to protect recipients of welfare, similar to how private property in the Constitution historically operated.[182] Similarly, at the House hearing, Reich emphasized that constitutional rights were at risk in the automatic data processing by the centralized computer

---

[175] *See* O'Mara, *supra* note 162.

[176] *Id.*; MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 123 (2019).

[177] *Computer and Invasion of Privacy Hearings*, *supra* note 162, at 10 (statement of Vance Packard).

[178] *Id.* at 13.

[179] *Id.* at 11.

[180] Rodger D. Citron, *Introduction to the Conference: Commemorating the Life and Legacy of Charles A. Reich*, 36 TOURO L. REV. 707 (2020).

[181] *See, e.g.*, Charles A. Reich, *Midnight Welfare Searches and the Social Security Act*, 72 YALE L.J. 1347 (1963); Charles A. Reich, *The New Property*, 73 YALE L.J. 733, 761 (1964); Charles A. Reich, *Individual Rights and Social Welfare: The Emerging Legal Issues*, 74 YALE L.J. 1245, 1248 (1965); Charles A. Reich, *The New Property After 25 Years*, 24 U.S.F. L. REV. 223, 242 (1990). In subsequent years, this issue gained more attention in the discussion of privacy. *See* Joel F. Handler & Margaret K. Rosenheim, *Privacy in Welfare: Public Assistance and Juvenile Justice*, 31 LAW & CONTEMP. PROBS. 377, 377–78 (1966).

[182] Reich, *The New Property*, *supra* note 181, at 778.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

system.[183] There were two reasons for this: one was that information may not be accurate, as "any time bad information is supplied about an individual, his legal rights are invaded at that moment."[184] The other was that the data processing was secret: "The individual does not know what I have said about him. He does not know what is in the computer's file. He does not know what the computer says about him. He does not know what judgments people make on the basis of that."[185] Reich asserted that, "[i]t seems to me without question a denial of due process of law to send forth bad information about a person in secret in that way."[186] "It is in this," Reich concluded, "that I see the essence of the evil of the automatic data center."[187]

In August 1968, the House Subcommittee produced a report, concluding that "a grave threat to the constitutional guarantees exists in the National Data Bank concept."[188]

2. The Senate Hearings in 1967–1968

The 1967–1968 Senate hearings on "Computer Privacy" included Carl Kaysen, Charles Zwick,[189] and the critics Alan F. Westin, then a professor at Columbia University,[190] and Arthur R. Miller, a law professor from the University of Michigan.[191] Since 1962, Westin had served as the director of a research project, "The Impact of Science and Technology on Privacy" sponsored by the Special Committee on Science and Law of the Association of the Bar of the City of New York.[192] By the time he came to the Senate hearing, Westin had researched the computer and its threats to privacy, including authoring a book, *Privacy and*

[183] *Computer and Invasion of Privacy Hearings*, *supra* note 162, at 28 (statement of Prof. Charles A. Reich).

[184] *Id.*

[185] *Id.*

[186] *Id.* at 29.

[187] *Id.*

[188] H.R. REP. NO. 90-1842, at 5 (1968).

[189] *Computer Privacy Hearings*, *supra* note 169, at iii.

[190] *Id.* at 277 (statement of Prof. Alan Westin, Columbia University, Department of Public Law and Government).

[191] *Id.* at 66 (statement of Arthur R. Miller, Professor of Law, University of Michigan).

[192] *Id.* at 277 (statement of Prof. Alan Westin).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Freedom.[193] Westin also maintained close ties with ACLU: he chaired the Privacy Committee of the ACLU in addition to serving on the latter's national board of directors.[194] At the Senate hearing in February 1968, Westin was critical of the national data center proposals, calling them "not properly matured and carefully considered."[195] Westin characterized the privacy issue in computerized data systems as a "due process" problem.[196] Westin's statement at the Senate hearing included a definition of privacy that would become the central theme of the privacy revolution:

> The essence of privacy, expressed in virtually every legal, sociological and psychological definition, is the right of the individual to determine those to whom he will reveal personal information about himself, how much he will reveal, and at what time. Applied to computerized data systems, the central issue of privacy is whether certain kinds of information about an individual that he chooses to give to one person, organization or government agency should be allowed to circulate to others without the individual's knowledge and consent.[197]

[193] ALAN F. WESTIN, PRIVACY AND FREEDOM (1967). The book was based on articles Westin published during this period. *See* Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I—The Current Impact of Surveillance on Privacy*, 66 COLUM. L. REV. 1003, 1004 (1966); Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part II—Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66 COLUM. L. REV. 1205, 1205–06 (1966) [hereinafter Westin, *Part II*]. In his opening statement, Senator Long referred to Westin's book, recognizing him as "the leading authority in the area of privacy and freedom." *Computer Privacy Hearings*, *supra* note 169, at 277 (statement of Sen. Edward V. Long). Senator Long's remarks indicated that the book might have been one of the reasons that Westin was invited to the Senate hearings. *Id.*

[194] *Computer Privacy Hearings*, *supra* note 169, at 278 (statement of Prof. Alan Westin).

[195] *Id.*

[196] *Id.* at 280.

[197] *Id.* This conceptualization came from one of Westin's earlier articles. *See* Westin, *Part II*, *supra* note 193, at 1210 ("Privacy means, in part, that individuals and organizations are usually permitted to determine for themselves what they want to keep private and what they want—or need—to reveal."). Similar efforts to redefine privacy in the same period can also be found in Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves.") (emphasis in original). Charles Fried attributed this notion of privacy partially to sociologist Erving Goffman. *Id.* at 485 n.18 ("Erving Goffman has suggested to me in conversation that new methods of data storage and retrieval pose a threat to privacy in that it is possible to make readily accessible information about a person's remote and forgotten past.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In order to build safeguards in the computerized data systems, Westin called for a full-scale congressional inquiry into the specific safeguards for privacy.[198]

In his testimony, Arthur R. Miller rejected the sharp line between a statistical data center and an intelligence data center.[199] Miller highlighted special risks to individual privacy in a centralized computer system characterized by a self-perpetuating tendency.[200] Miller further classified the risks into five categories: first, errors in the data are inevitable; second, the computer is not infallible, and machine malfunction may distort the information gathered; third, the risk of misuse of information by the people working with the information; fourth, there will be greater tendency to use information for the purpose totally unrelated to the purpose for which it was collected; and fifth, there will be an increase in the tendency of those governmental agencies to snoop.[201] Like Westin, Miller suggested that safeguards should be built into the system if a national data center were established.[202] First, Miller addressed the scope of what data should be permitted into the data system: "It strikes me that psychiatric, medical, evaluative material, and nonfactual data do not belong in a Federal Data Center or in the computer files of any governmental agency . . . ."[203] Second, Miller suggested that "whatever information is put into the Data Center should be made available periodically to every citizen."[204] Third, Miller proposed that "anyone trying to gain access to or record information in any governmental data bank should identify himself."[205] Fourth, Miller concluded that control of the national data center should lie outside of any existing agencies and said, "[t]he key is insuring that it remains independent."[206]

---

[198] *Computer Privacy Hearings*, *supra* note 169, at 281 (statement of Prof. Alan Westin).

[199] *Id.* at 67 (statement of Prof. Arthur R. Miller).

[200] *Id.* at 68 ("As our capacity to ingest or collect information increases, the more information we want. Consequently, as the Government's capacity to report, collect, disseminate, analyze, and manipulate information has increased, the Government has tended to gather more information.").

[201] *Id.*

[202] *Id.* at 71.

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.* at 85. *See generally* Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1092–93 (1969); Richard Ruggles, John de J. Pemberton, Jr. & Arthur R. Miller, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 219 (1968); Arthur R. Miller, *The Dossier Society*, 1971 U. ILL. L.F. 154, 166

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

3. The Senate Hearing in February–March 1971

By the time of the February–March 1971 Senate hearings on "Federal Data Banks," the tide had changed. Alan Westin assessed in February 1968 that most of computer specialists in the United States "very realistically think the National Data Center is probably dead."[207] Criticism became more visible after the Senate hearings in February 1968. The American Bar Foundation funded a large research project on the matter, which led to an article published in the *UCLA Law Review* in 1968.[208] In the same year, the *Harvard Law Review* also published a student note critiquing the National Data Bank proposals.[209] In June 1970, the ACLU adopted a resolution at its Biennial Conference on "Data Storage, Collection and Dissemination."[210] Thus, the focus of the 1971 Senate hearings was more on safeguards, including collection of empirical information regarding the safeguards in practice, and the design of a possible regulatory framework.[211]

In his testimony on February 23, 1971, Arthur R. Miller discussed the legal aspects of privacy protection.[212] Miller called on Congress to act, stating, "I think it is now time for the Congress to begin to lay down new legislative guidelines about the significance of individual privacy and file confidentiality in this Nation."[213] Miller noted that the common law of privacy—developed after the Warren-Brandeis article—had become outdated by now: "The entire concept of personal privacy as developed by the courts has been in reaction to the media of mass communication."[214] However, Miller argued, the situation had changed:

(1971); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 233 (1971); Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 11 (1972).

[207] *Computer Privacy Hearings*, *supra* note 169, at 282 (statement of Prof. Alan Westin).

[208] *The Computerization of Government Files: What Impact on the Individual*, 15 UCLA L. REV. 1377 (1968).

[209] Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 400–01 (1968).

[210] *Federal Data Banks Hearings*, *supra* note 96, at 64–65.

[211] *Id.* at 1.

[212] *Id.* at 8 (statement of Prof. Arthur R. Miller).

[213] *Id.* at 18.

[214] *Id.* at 17.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

> You are not dealing with the newspapers or radio and television. You are dealing with records that are kept and stored in electronic form in the bowels of some Federal agency or some State agency or some corporation or some university, of which the citizen simply has no knowledge. In other words, the person most concerned with the information, the person who will be affected by others seeing and acting on it, often has the least access to it. The law of privacy as we know it today simply has not developed or reacted to this problem.[215]

Miller also called on Congress to consider a regulatory entity to solve the issue: "I think it is time for the Congress to begin to think of putting a neutral third force into the informational environment within the Federal Government and perhaps even in the private sector . . . ."[216] In response to Senator Hruska's question, Miller replied, "I would prefer to call it something like an informational ombudsman," or an "auditor concept."[217]

Alan F. Westin, who spoke on March 15, totally echoed Miller's statement when he told the Senate, "what we all would seek as part of our right to privacy is the capacity to control uncontrolled uses of the information, the permission that we give to one person for one purpose should not justify uses that we don't know anything about and have not consented to."[218] Westin led a project of the Computer Science and Engineering Board of the National Academy of Sciences,[219] which led to a survey in 1971.[220] His other book, *Databanks in a Free Society*, was published in 1972.[221]

Consensus was emerging among privacy advocates at the February–March 1971 Senate hearings.[222] Mr. Burt Neuborne, speaking on behalf of the ACLU on February 23, suggested three legislative areas that ought to be explored in developing

---

[215] *Id.*

[216] *Id.* at 18.

[217] *Id.* at 19.

[218] *Id.* at 826 (statement of Prof. Alan F. Westin).

[219] *Id.* at 828.

[220] INFORMATION TECHNOLOGY IN A DEMOCRACY (Alan F. Westin ed., 1971).

[221] ALAN F. WESTIN & MICHAEL A. BAKER, NAT'L ACAD. OF SCI., DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).

[222] *See Federal Data Banks Hearings*, *supra* note 96, at 46–56 (statement of Burt Neuborne, Attorney, American Civil Liberties Union).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

a set of substantive controls in data gathering.[223] The first area was "absolute prohibition of the gathering of information dealing with lawful political activities"; the second area was a "statutory ban on the maintenance or collection of hearsay or anonymous derogatory information"; and the third area was the "expungement" of "arrest records."[224] On procedural safeguards, Neuborne suggested the following: (1) "notice must be given to a person that a dossier is being compiled"; (2) advanced notice must be given before a government agency is permitted to disseminate information about an individual; and (3) there must be some procedure to permit a person to correct inaccurate or improper information held by the government.[225] Ms. Hope Eastman, Acting Director of ACLU's Washington, DC, office added that "[t]he ACLU believes that giving the individual a right of access to his files is the most effective way of policing what the Government does."[226]

In sum, by 1971, a consensus that the data subject must be given some control over the data about herself had been formed in the circle of privacy advocates organized around the Senate's February–March hearings.[227] From the July 1966 House hearings to the 1971 Senate hearings, a notion that can be characterized as an American Bill of Rights on data evolved from a theoretical claim to a policy demand.

C. The Legislative Response

The legislative initiative towards the 1974 Act began with the Executive branch. It started in January 1969, when the Committee on Scientific and Technical Information ("COSATI") of the Federal Council of Science and Technology established a panel on Legal Aspects of Information Systems.[228] In June 1972, the

[223] *Id.* at 46, 49.

[224] *Id.* at 49.

[225] *Id.* at 52–53.

[226] *Id.* at 56 (statement of Hope Eastman, Acting Director, American Civil Liberties Union).

[227] This notion of privacy was not limited to the testimonies in the United States Congress. *See, e.g.*, Vern Countryman, *Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEX. L. REV. 837 (1971); SHIRLEY M. HUFSTEDLER, THE DIRECTIONS AND MISDIRECTIONS OF A CONSTITUTIONAL RIGHT OF PRIVACY (1971); PRIVACY (J. Roland Pennock & John W. Chapman eds., 1971).

[228] Robert P. Bigelow, *The Privacy Act of 1974*, PRAC. LAW, Sept. 1, 1975, at 15, 16. The Panel was composed of "nationally recognized lawyers, economists, engineers, scientists, and information systems specialists," including Arthur R. Miller, COMM. ON SCI. AND TECH. INFO. OF THE FED. COUNCIL FOR SCI. AND TECH., LEGAL ASPECTS OF COMPUTERIZED INFORMATION SYSTEMS app. at 5, 8 (1972) [hereinafter LEGAL ASPECTS]. The Panel chose seven areas to work on: (1) "[t]he right of entry and access to information systems"; (2) "[t]he Freedom of Information Act"; (3) "[t]he right of privacy"; (4) "[a]nti-

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

COSATI Panel sponsored a symposium in Washington, DC, where a set of principles for the guidance of the federal government was proposed.[229] On the topic of privacy, Arthur R. Miller noted two major concerns: "(1) the growing loss of privacy; i.e., the loss of a person's ability to control the flow of information about himself; and (2) an increase in social alienation as a result of increased government data collection, use, and surveillance."[230] Miller suggested that "[p]rocedural methods for origination, handling, dissemination, and elimination of data" were needed to balance legitimate use of data and privacy concerns.[231] For this reason, Miller suggested that federal agencies should have an obligation to consider the following four aspects of data: (1) "the legitimacy of the need for data"; (2) "the effectiveness of disclosure to the citizen"; (3) "repetitiveness in data collection"; and (4) "confidentiality."[232] After the symposium, the Panel further revised the papers and integrated ideas in a report in September 1972.[233] The report fully embraced Miller's suggestions and elaborated in more detail on the principles.[234] Specifically, the report recommended that "[t]he use of coercion or intimidation in the course of gathering information must be avoided."[235]

In the meantime, Elliot L. Richardson, Secretary of Health, Education and Welfare, established the Secretary's Advisory Committee on Automated Personal Data Systems in February 1972.[236] One year earlier, Secretary Richardson was more enthusiastic about using the SSN as a universal identifier.[237] In February 1972,

---

trust issues"; (5) "[p]roprietary rights"; (6) "[c]opyright issues in the United States"; and (7) "[t]he international copyright situation." *Id.* at 5.

[229] LEGAL ASPECTS, *supra* note 228, at 5.

[230] *Id.* at 8.

[231] *Id.*

[232] *Id.*

[233] *Id.*

[234] *Id.* at 29–32.

[235] *Id.* at 31.

[236] RECORDS, COMPUTERS, AND RIGHTS REPORT, *supra* note 13, at 147. The Advisory Committee was composed of federal and state officials, industry leaders, and scholars, including two academic lawyers: Professor Arthur R. Miller of Harvard Law School and Professor Layman E. Allen from the University of Michigan. *See id.* at xii-xiii.

[237] *Federal Data Banks Hearings*, *supra* note 96, at 785 (statement of Hon. Elliot L. Richardson, Secretary of Health, Education and Welfare) ("The Department of Health, Education, and Welfare is now

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Secretary Richardson asked his Advisory Committee to analyze and make recommendations identifying "[h]armful consequences that may result from using automated personal data systems," and "[s]afeguards that might protect against potentially harmful consequences."[238] In July 1973, the Advisory Committee issued a report titled *Records, Computers and the Rights of Citizens*.[239] The report called for a "[r]edefinition of the [c]oncept of [p]ersonal [p]rivacy."[240] It embraced the frameworks of Alan Westin, Charles Fried, and others, through the lens of control:

> A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it.[241]

For this purpose, the report recommended five fundamental principles of "fair information practice": (1) openness, (2) individual access, (3) collection limitation, (4) use and disclosure limitations, and (5) information management.[242] These principles became the very foundation of the 1974 Act.

---

undertaking to develop policy recommendations on the use of the Social Security number as a universal identifier.").

[238] RECORDS, COMPUTERS, AND RIGHTS REPORT, *supra* note 13, at ix, 147. Richardson's contemporary, *New York Times* journalist David Burnham, noted Richardson's "zigs and zags" on the question of privacy. *See* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE: THE THREAT TO OUR FREEDOMS, OUR ETHICS AND OUR DEMOCRATIC PROCESS 197 (1983).

[239] RECORDS, COMPUTERS, AND RIGHTS REPORT, *supra* note 13, at vi, xix–xxxv.

[240] *Id.* at 38.

[241] *Id.* at 41.

[242] *Id.*

> There must be no personal-data record-keeping systems whose very existence is secret[; t]here must be a way for an individual to find out what information about him is in a record and how it is used[; t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent[; t]here must be a way for an individual to correct or amend a record of identifiable information about him[; a]ny organization creating, maintaining, using, or disseminating records of

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Furthermore, the report understood the crucial role of SSNs.[243] It noted that "[t]he Committee paid particular attention to the dangers implicit in the drift of the social security number toward becoming an all-purpose personal identifier,"[244] recognizing that "[a] persistent source of public concern is that the social security number will be used to assemble dossiers on individuals from fragments of data in widely dispersed systems."[245] The report recommended that "use of the social security number be limited to Federal programs that have a special Federal legislative mandate to use the SSN, and that new legislation be enacted to give an individual the right to refuse to disclose his SSN under all other circumstances."[246]

Shortly after the 1973 Advisory Committee report, a number of legislative bills were introduced.[247] On May 1, 1974, Senators Ervin, Percy, and Muskie introduced S. 3418 to the U.S. Senate,[248] which was used as the foundation for deliberations leading to the final 1974 Act.[249] In June 1974, a four-year study led by Senator Ervin's Subcommittee on Constitutional Rights, *Federal Data Banks and Constitutional Rights*, was finally published.[250] It was a six-volume, comprehensive survey of fifty-four federal government agencies' data practices in 858 data banks

---

> identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Id.

[243] *Id.* at xix, xxi.

[244] *Id.* at xix.

[245] *Id.* at xxi.

[246] *Id.* at xxii.

[247] *See* S. 2542, 93d Cong. (1973), *reprinted in* STAFF OF S. COMM. ON GOV'T OPERATIONS & H. SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RTS. OF THE H. COMM. ON GOV'T OPERATIONS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418, PUBLIC LAW 93-579: SOURCE BOOK ON PRIVACY 584 (Joint Comm. Print 1976) [hereinafter SOURCE BOOK ON PRIVACY]; S. 2810, 93d Cong., *reprinted in* SOURCE BOOK ON PRIVACY, at 591; S. 3116, 93d Cong., *reprinted in* SOURCE BOOK ON PRIVACY, at 651.

[248] *Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Ad Hoc Subcomm. on Priv. and Info. Sys. of the S. Comm. on Gov't Operations and the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary*, 93d Cong. 357–76 (1974).

[249] Jerome J. Hanus & Harold C. Relyea, *A Policy Assessment of the Privacy Act of 1974*, 25 AM. U. L. REV. 555, 572–73 (1976).

[250] STAFF OF SUBCOMM. ON CONST. RTS. OF THE S. COMM. ON THE JUDICIARY, 93D CONG., FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS iii (Comm. Print 1974).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

they operated.[251] Senator Ervin, who also chaired the U.S. Senate Select Committee on Presidential Campaign Activities ("Watergate Committee"),[252] pushed through the bill on his last day of service in the Senate, and on December 31, 1974, the Privacy Act was passed in Congress.[253]

The 1974 Act recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[254] The statement reflected the way Senator Ervin envisioned the Act as a safeguard to the fundamental values in the Constitution,[255] short of a constitutional amendment. The Act contained basic rules limiting the collection of data,[256] limiting the use and sharing of data,[257] enabling access to and correction of data,[258] and providing civil and criminal remedies for violations of these statutory rights.[259] It was essentially an American Bill of Rights for the computer age. However, there is no doubt the 1974 Act was a political compromise. It had two fundamental weaknesses in its design. First, it contained generous exemptions to intelligence and law enforcement agencies.[260] Second, it chose to establish a Privacy Protection Study Commission, whose task was to study data banks and develop standards and procedures for the protection of data.[261] The Commission had no enforcement power.[262]

---

[251] *Id.* at iv.

[252] Hanus & Relyea, *supra* note 249, at 570–71.

[253] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a). For commentary on the Act, see *The Privacy Act of 1974: An Overview and Critique*, 1976 WASH. U. L. REV. 667 (1976); James Beverage, *The Privacy Act of 1974: An Overview*, 1976 DUKE L.J. 301 (1976); and Hanus & Relyea, *supra* note 249. *See also ERVIN, Samuel James, Jr.*, BIOGRAPHICAL DIRECTORY OF THE U.S. CONG., https://bioguide.congress.gov/search/bio/E000211 [https://perma.cc/US4H-E9WK] (last visited Sept. 5, 2024).

[254] Privacy Act of 1974 § 2(a)(4), at 1896.

[255] Sam J. Ervin, Jr., *The Computer vs. Our Constitution*, 1 BARRISTER 14, 16 (1974).

[256] Privacy Act of 1974 § 3(e), at 1899.

[257] *Id.* § 3(b), at 1897.

[258] *Id.* § 3(d), at 1898.

[259] *Id.* § 3(g)(1), (i)(1), at 1901–02.

[260] *Id.* § 3(j), (k), at 1902–03.

[261] *Id.* § 5(a)(1), (b)(1), at 1905–06.

[262] *See id.* § 5(b)(2), at 1906.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

D. Parallel Developments in Europe and Commonwealth Countries

As in the United States, computers were introduced into the United Kingdom ("UK") in the late 1950s: the Board of Trade started using an Elliot 405 in 1957, and the Ministry of Pensions and National Insurance installed a Leo II computer in 1959.[263] "By 1958 seven UK government departments had introduced programmable electronic machines, the number of which rose to 45 by 1965."[264] This was quickly followed by other countries across Europe.[265] *The New York Times* reported in April 1971 that as files were computerized, concerns about privacy became widespread, and countries like Sweden, Britain and Denmark had set up committees to explore the protection of privacy by legislation.[266] By 1974, a number of European countries had also passed their first generation of data protection laws, embracing the same fundamental principles listed in the table below and covering both governmental agencies and private entities.

1. Continental Europe

Table: European Data Protection Laws[267]

[263] Jon Agar, *What Difference Did Computers Make?*, 36 SOC. STUD. SCI. 869, 881–82 (2006) [hereinafter Agar, *What Difference Did Computers Make?*]; JON AGAR, THE GOVERNMENT MACHINE: A REVOLUTIONARY HISTORY OF THE COMPUTER 300 (2003).

[264] Agar, *What Difference Did Computers Make?*, *supra* note 263, at 879. The military and intelligence departments of the British government used computers from the World War II period. *See* Jon Agar, *Putting the Spooks Back In? The UK Secret State and the History of Computing*, 51 INFO. & CULTURE: J. HISTORY 102 (2016).

[265] *See* JAMES W. CORTADA, THE DIGITAL FLOOD: THE DIFFUSION OF INFORMATION TECHNOLOGY ACROSS THE U.S., EUROPE, AND ASIA 145–194 (2012).

[266] Bernard Weinraub, *Computer Invasion of Personal Privacy Worries Europeans*, N.Y. TIMES, Apr. 17, 1971, at 1.

[267] Datenschutzgesetz [Data Protection Act], Oct. 7, 1970, GESETZ-UND VERORDNUNGSBLATT FÜR DAS LAND HESSEN at 625–627 [https://perma.cc/9UEK-KF2H] (Ger.); Gesetz gegen miBbrauchliche Datennutzung [Landesdatenschutzgesetz—LdatG] [State Data Protection Act], Jan. 24, 1974, Gesetz- und Verordnungsblatt für das Rheinland-Pfalz at 3, 31; Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten [Datenschutzgesetz—DSG] [Data Protection Act of Oct. 18, 1978] BUNDESGESETZBLATT FÜR DIE REPUBLIK ÖSTERREICH No. 565/1978, at 3619–31 [https://perma.cc/J2KG-AXBW] (Austria); SELECTED FOREIGN NATIONAL DATA PROTECTION LAWS AND BILLS 3–80 (Charles K. Wilk ed., 1978).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Law	Collection of Data	Use of Data	Accuracy check	Agency	Remedy
Land Hessen (West Germany) Data Protection Act, Oct. 7, 1970	The right to information of data subjects (§ 6).	Use of data limited by law (§ 3).	Right to correct inaccuracy (§ 4).	Data Protection Commissioner, *Land* Parliament (§ 7).	Unspecified offense committed upon violation of § 3 (§ 16).
Swedish Data Act, May 11, 1973	By a permit system (§ 2); notification upon request (§ 10).	Use of data limited by law (§ 11).	The right to correct inaccuracy (§ 8), and incompleteness (§ 9).	Data Inspection Board, having the powers of issuing permits (§ 3), supervision (§§ 15-19), and enforcement (§ 6).	Criminal liability (§§ 20–21).
Land Rhineland-Palatinate (West Germany), Data Protection Act, Jan. 24, 1974	The right to information of data subjects (§ 11).	Use and retention of data (§ 4).	The right to correction or erasure (§ 12).	Data Protection Committee, its power of supervision (§ 6).	Civil remedy for damages (§ 13); criminal liability (§ 15).
Austria, Data Protection Act, Oct. 18, 1978	Statutory authorization required (§ 6); data banks rules (§ 9).	Transfer of data (§§ 13, 18–19).	The obligation to rectify or erase of incorrect data (§§ 12, 26–27).	Data Protection Commission (§ 10); the power to hear and decide complaints (§ 14); annual reports (§ 23).	Civil liabilities (§ 28).
West Germany, Federal Data Protection Law BDSG, Jan. 27, 1977	Permission is required (§ 3); the right to information (§ 4); notice concerning stored data (§ 12); storage of data in the private sector (§ 23); the right to information (§ 26).	Use and transfer of data limited by purpose (§ 5); transmission of data in the public sector (§§ 10, 11); in the private sector (§ 24).	The right to correct data (§ 4); correction and deletion of data in the public sector (§ 14); in the private sector (§ 27).	Federal Commissioner for Data Protection (§ 17); supervision powers (§ 19); the power to hear complaints (§ 20); supervision in the private sector (§ 30).	Criminal liability (§ 41); fine (§ 42).
France, Law No. 78-17, Jan. 6, 1978	Statutory authorization (Art. 15); the right to know (Art. 3); data subject must be informed of their rights (Art. 27).	Storage of data (Art. 28).	Right of access (Art. 34); the right to require correction (Art. 36).	National Commission on Data Processing and Liberties (Art. 6); supervision powers (Art. 21).	Criminal liabilities (Arts. 41–44).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

A major driving force was the International Commission of Jurists ("ICJ"), a nongovernmental organization of lawyers, judges and teachers of law established in 1953 in West Berlin.[268] In the years following World War II, the ICJ became a powerful advocate for the rule of law and human rights. The ICJ's "Nordic Conference on the Right to Privacy" in 1967 defined privacy as "the right to be let alone to live one's own life with the minimum degree of interference."[269] However, one characteristic of the Nordic Conference notion of privacy differed from that in the American notion. It went beyond tort law by drawing from elements of international law and constitutional law. The Nordic Conference urged that the right of privacy be "recognized as a fundamental right of mankind."[270] As a fundamental right, "[i]t protects the individual against public authorities, the public in general and other individuals."[271]

At the time of the Nordic Conference, the impact of the computer was not yet fully felt in Europe.[272] According to a report by the United Nations Educational, Scientific and Cultural Organization ("UNESCO"), "it was not until the publication in 1967 of Westin's book . . . that it began to attract attention elsewhere."[273] The UNESCO report highlighted the profound challenges of the computer and data banks to privacy.[274] The Organisation for Economic Co-operation and Development

---

[268] LUCIAN G. WEERAMANTRY, THE INTERNATIONAL COMMISSION OF JURISTS: THE PIONEERING YEARS 3–5 (2000); GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 39 (2014).

[269] INT'L COMM. OF JURISTS, NORDIC CONFERENCE ON THE RIGHT OF PRIVACY 1–2 (1967).

[270] *Id.* at 2.

[271] *Id.* The Nordic Conference was held in the context of Article 12 of the Universal Declaration of Human Rights, Article 17 of the United Nations Covenant on Civil and Political Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Id.* at 1.

[272] "There is one aspect of privacy which was not considered in any detail at the Stockholm conference, but which is now seen by many people to constitute, potentially, the greatest threat of all, namely the collection, storage, and dissemination of personal information by means of computers or 'data banks.'" *The Legal Protection of Privacy: A Comparative Survey of Ten Countries by the International Commission of Jurists*, 24 INT'L SOC. SCI. J. 417, 420 (1972).

[273] *Id.*

[274] *Id.* at 428.

> People have become accustomed to making a lot of information about themselves available for particular purposes. Each item of information does not in itself reveal very much and persons are willing to disclose it, confident that those to whom it

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

("OECD") at its Ministerial Meeting on Science in March 1968, recognized the development of computer technology.[275] An Expert Group on Computer Utilization was set up by the Committee for Science Policy.[276] In 1971, a study of computerized data banks was published by OECD.[277] The study suggested the orientation of the OECD when it made this comment on privacy:

> [I]t is important to look at privacy, not so much from the aspect of the extent to which the citizen has a right to be left alone, as from the aspect of what are the justifiable needs of public administration regarding data on individuals. In the latter case the burden of proof as to what extent data has to be collected and transferred is on the public administration and not on the citizen.[278]

In September 1973 and September 1974, the Council of Europe's Committee of Ministers adopted two resolutions on data protection: the first one, Resolution (73) 22, established principles of data protection for the private sectors;[279] and the second one, Resolution (74) 29, addressed the public sectors.[280]

> is given will use it only for the purpose for which it is intended. If one thinks about the matter one may also conclude that it would not be practical for anyone to bring together the different items of information in such a way as would enable a picture, however distorted, to be constructed of one's private life and activities. All that is now changed by the computer.

Id.

[275] ORG. FOR ECON. COOP. & DEV., *Gaps in Technology Between Member Countries: General Report*, *in* THIRD MINISTERIAL MEETING ON SCIENCE OF OECD COUNTRIES: DOCUMENTS FOR DISCUSSION 1, 9 (1968).

[276] *Id.* at 39.

[277] UWE THOMAS, COMPUTERIZED DATA BANKS IN PUBLIC ADMINISTRATION: TRENDS AND POLICIES ISSUES (1971).

[278] *Id.* at 61.

[279] Council of Europe Committee of Ministers, *On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector: Resolution (73) 22*, COUNCIL OF EUR. (Sept. 26, 1973), https://rm.coe.int/1680502830 [https://perma.cc/84DC-U94V].

[280] Council of Europe Committee of Ministers, *On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector: Resolution (74) 29*, COUNCIL OF EUR. (Sept. 20, 1974), https://rm.coe.int/16804d1c51 [https://perma.cc/6ZSH-LWN5].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

2. Commonwealth Countries

The British Section of the International Commission of Jurists ("Justice") published its report in January 1970 called *Privacy and the Law* (the "Justice Report").[281] The Justice Report acknowledged that English law had not recognized a general right of privacy,[282] and it called for creating a new statutory tort for the protection of privacy.[283] It even prepared a draft Right of Privacy Bill.[284] While it took notice of the computerized data banks,[285] the Justice Report did not fully grasp the challenge posed by them.

However, concerns about the data banks became clearer in Britain in 1970. In their book *The Data Bank Society*, Malcolm Warner and Michael Stone recognized that "[p]ublic opinion in Britain has until recently been complacent, even somnolent, about the implications of computer technology."[286] Civic groups like the National Council for Civil Liberties became more vocal on privacy.[287] The draft "Right of Privacy Bill" prepared by Justice was picked up by Mr. Brian Walden, MP, who brought it to the House of Commons.[288] With the government's opposition, the Bill did not succeed in the second reading.[289] Instead, a Committee on Privacy, chaired by Sir Kenneth Younger, was set up in April 1970 to study the issue (the "Younger

[281] JUSTICE—BRITISH SECTION OF THE INT'L COMM'N OF JURISTS, PRIVACY AND THE LAW (1970) [hereinafter JUSTICE REPORT]. For commentary, see G.D.S. Taylor, *Privacy and the Public*, 34 MOD. L. REV. 288 (May 1971).

[282] JUSTICE REPORT, *supra* note 281, at 2 ("[I]t is noteworthy that English law does not at present recognize any general right to privacy. The law protects a man's person, it protects his property, it protects his reputation, but it does not specifically protect his privacy.").

[283] *Id.* at 35 ("We have therefore reached the conclusion and recommend that the right method of providing for the protection of privacy in general is the creation of a new statutory tort of 'infringement of privacy.'").

[284] *Id.* at 59–62.

[285] *Id.* at 29, 34, 42, 54.

[286] MALCOLM WARNER & MICHAEL STONE, THE DATA BANK SOCIETY: ORGANIZATIONS, COMPUTERS AND SOCIAL FREEDOM 81 (1970).

[287] *See* PRIVACY, COMPUTERS AND YOU 9 (B.C. Rowe ed., 1972). For the history and activities of the NCCL, see MARK LILLY, THE NATIONAL COUNCIL FOR CIVIL LIBERTIES: THE FIRST FIFTY YEARS (1984).

[288] HC Deb (23 Jan. 1970) (794) col. 861–959 (U.K.), https://api.parliament.uk/historic-hansard/commons/1970/jan/23/right-of-privacy-bill [https://perma.cc/S2ER-CFCD].

[289] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Committee").[290] However, the mandate for the Younger Committee excluded privacy in the public sectors.[291] This limitation was set when the British Ministry of Social Security was about to computerize thirty million social security records and the Post Office was prepared to launch its National Data Processing Service.[292] It only shows that the executive branch of the British government was not ready for comprehensive data regulation. Despite the limitations, the Younger Committee's report embraced a broader notion of privacy, which included "the right to determine for oneself how and to what extent information about oneself is communicated to others."[293]

In Canada, similar practices of electronic wiretapping and eavesdropping were raising concerns in the mid-1960s.[294] In April 1971, the Departments of Communications and Justice established a task force on privacy and computers, and one year later, it issued a report titled *Privacy and Computers*.[295] The task force report had an interesting discussion of the difference between traditional common law tort of defamation that protected reputation, on the one hand, and privacy understood as personal integrity:

> A man's reputation is essentially based on the assessment and esteem of others. His personal integrity is fundamentally a matter internal to himself and relates to his self-esteem. Reputation is legally recognized to be injured by falsehood or malice. Personal integrity may be injured merely by facts about an individual passing out of his control.[296]

---

[290] Two years later, the report—known as the Younger Report—was presented to the Parliament in July 1972. *See* KENNETH YOUNGER, REPORT OF THE COMMITTEE ON PRIVACY (1972) [hereinafter YOUNGER REPORT]; *see also* HL Deb (6 June 1973) (343) col. 104–78 (U.K.), https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report [https://perma.cc/U4EW-3GCS]. For commentary, see Gerald Dworkin, *The Younger Committee Report on Privacy*, 36 MOD. L. REV. 399 (1973).

[291] YOUNGER REPORT, *supra* note 290, at 2.

[292] WARNER & STONE, *supra* note 286, at 103.

[293] YOUNGER REPORT, *supra* note 290, at 10.

[294] Stanley M. Beck, *Electronic Surveillance and the Administration of Criminal Justice*, 46 CAN. BAR REV. 643, 644 (Dec. 1968) (detailing the extensive use of listening devices).

[295] PRIVACY AND COMPUTERS: A REPORT BY A TASK FORCE ESTABLISHED JOINTLY BY DEPARTMENT OF COMMUNICATIONS/DEPARTMENT OF JUSTICE (1972).

[296] *Id.* at 132.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In 1973, the Canadian Privacy and Computer Task Force also published a report on data banks.[297] The conceptual transformation of privacy rights in commonwealth countries took a longer time compared to those in continental Europe. Canada, like Great Britain and Australia, did not start drafting its data protection legislation until the 1980s.[298]

In sum, the Privacy Act of 1974 was a catalyst in the 1970s toward leading a revolutionary change to the notion of privacy. Its central thesis—empowering the individual by giving her control of the data about herself, embodied in the five fundamental principles—quickly spread throughout western democracies as they entered into the computer age. However, in the decades after the 1974 Act, the revolution was severely undercut in the United States, while it continued elsewhere.

III. UNDOING THE REVOLUTION: SSNS IN COURTS

During the deliberations that led to the 1974 Act in the United States, neither congressional leaders nor privacy advocates expected the judiciary to lead the privacy revolution.[299] However, what they did not anticipate was that the courts, in the decades following the passage of the 1974 Act, would undo the revolution by imposing a tort law theory of privacy on the law.[300] This happened in cases where specific clauses of the 1974 Act were interpreted and constitutional issues were raised.

A. The Privacy Act of 1974 in Courts

1. Disclosure of Personal Records

In the initial years after the Privacy Act took effect in 1974, litigation centered on disclosure. Section 3(b) of the Act prohibits disclosure of "any record."[301] The

[297] KENNETH KATZ, REGULATION OF FEDERAL DATA BANKS: A STUDY FOR THE PRIVACY AND COMPUTERS TASK FORCE (1973).

[298] *See infra* Section IV.B.

[299] Alan F. Westin stated in 1971, "The courts have tended to shy away from the area of executive agency collection of surveillance information, on the theory . . . that this is purely interior to the executive branch until it is used either for indictment purposes or for regulatory purposes of some kind." *Federal Data Banks Hearings*, *supra* note 96, at 823.

[300] *See* Richard Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829 (1985).

[301] The Privacy Act of 1974, Section 3(b) provides: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

definition of "record,"[302] "systems of records,"[303] and "agency"[304] expanded so much so that in 1983 the Tenth Circuit asserted that the "distinction between information retrieved from a system of records and information independently acquired has been uniformly recognized by courts interpreting the Act."[305]

Section 3(g) of the Act provides civil remedies available to individuals with concerns about the privacy of their records, granting jurisdiction to federal district courts to rectify inaccuracy of the records and to award damages.[306] On damages, Section 3(g)(4) provides that for intentional or willful disclosure, the agency shall be liable to the individual for "actual damages" or no less than $1,000 plus the costs of the action, including reasonable attorney fees.[307] By design, Section (g)(4) was a legal remedy that empowered individuals to safeguard their privacy. In a series of cases, courts faced the question of what entitled a plaintiff to statutory recovery,

---

record pertains . . . ." Privacy Act of 1974, Pub. L. No. 93-579, § 3(b), 88 Stat. 1896, 1897 (1974) (codified as amended at 5 U.S.C. § 552a(b)).

[302] King v. Califano, 471 F. Supp. 180, 181 (D.D.C. 1979) ("[I]nformation alleged to have been divulged was a personal opinion stated from memory, not constituting a disclosure of a record within the meaning of the Privacy Act."); Jackson v. Veterans Admin., 503 F. Supp. 653, 656 (N.D. Ill. 1980) ("[I]n the present action . . . where only independently acquired information was disclosed, there is no violation of either the letter or the spirit of the [Privacy] Act."); Doyle v. Behan, 670 F.2d 535, 539 (5th Cir. 1982) (per curiam) ("[T]he information transmitted . . . was not retrieved from a system of agency records within the intendment of the Privacy Act."); Olberding v. U.S. Dep't of Def., 709 F.2d 621, 622 (8th Cir. 1983) (per curiam) (holding that disclosures did not violate the Privacy Act where the disclosures of information arose from the personal knowledge of an individual, and not from retrieval of information from the examining psychiatrist's report); Thomas v. U.S. Dep't of Energy, 719 F.2d 342, 345 (10th Cir. 1983) (holding that disclosure did not violate the Privacy Act where such information was derived from supervisor's independent knowledge and not from agency's systems of records, notwithstanding that records may have existed or that the supervisor may have known of their existence); Krowitz v. Dep't of Agric., 641 F. Supp. 1536,1544–45 (W.D. Mich. 1986) (holding that agency official's disclosures to his wife, friends, and staff concerning alleged employment problems of employee were not based upon retrieval of protected government records, but on official's own independent recollections and opinions, and thus did not violate Privacy Act), *aff'd*, 826 F.2d 1063 (6th Cir. 1987).

[303] Savarese v. U.S. Dep't of Health, 479 F. Supp. 304, 307 (N.D. Ga. 1979) ("[N]either the 'reading file' nor the 'program file' are systems of records under the Privacy Act's definitions."), *aff'd*, 620 F.2d 298 (5th Cir. 1980).

[304] Unt v. Aerospace Corp., 765 F.2d 1440, 1447 (9th Cir. 1985) ("The private right of civil action created by the [Privacy] Act is specifically limited to actions against agencies of the United States Government.").

[305] *Thomas*, 719 F.2d at 345.

[306] Privacy Act of 1974 § 3(g).

[307] *Id.* at § 3(g)(4)

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

specifically, whether a plaintiff who only alleged emotional distress or mental anguish was entitled to the statutory recovery under Section (g)(4).

The first such case that came to court was *Houston v. Department of Treasury*, in which an IRS agent alleged that certain information supplied to him by his supervisors concerning his case assignments was placed in his personnel file and later used against him in an adverse personnel action.[308] The United States District Court for the District of Columbia ruled that Section (g)(4) required "actual damages" for the plaintiff to be entitled to recovery.[309] This was the traditional tort law conception. For the court, a plaintiff's claims of reputation loss and emotional distress did not amount to "'out-of-pocket' losses."[310] Three years later, in *Fitzpatrick v. IRS*, the Eleventh Circuit came to the same conclusion.[311]

In the meantime, another way of reading Section (g)(4) soon emerged in the courts. In *Parks v. IRS*, a case in which the plaintiffs pleaded only "psychological damage or harm,"[312] the Tenth Circuit ruled that "plaintiffs . . . alleged viable claims for damages" under Section (g)(4).[313] Three years later, the Fifth Circuit came to a similar conclusion in *Johnson v. Department of Treasury*.[314] After a detailed examination of the legislative history, the Fifth Circuit explicitly rejected the policy concerns of limiting government liability.[315]

---

[308] 494 F. Supp. 24, 25 (D.D.C. 1979).

[309] *Id.* at 30 ("Although the term 'actual damages' is not defined in the Act, Congress, concerned about the drain on the treasury created by a rash of Privacy Act suits, indicated its intention to limit 'actual damages' to 'out-of-pocket' expenses.").

[310] *Id.* In the District of Columbia, similar cases include *Molerio v. FBI*, 749 F.2d 815 (D.C. Cir. 1984) and *Pope v. Bond*, 641 F. Supp. 489 (D.D.C. 1986).

[311] 665 F.2d 327, 328, 331 (11th Cir. 1982) ("[W]e hold that 'actual damages' as used in the Privacy Act permits recovery only for proven pecuniary losses and not for generalized mental injuries, loss of reputation, embarrassment or other non-quantifiable injuries.").

[312] 618 F.2d 677, 680 (10th Cir. 1980).

[313] *Id.* at 685.

[314] 700 F.2d 971, 972 (5th Cir. 1983) (holding that the plaintiff showed "proven and substantial physical and mental damage" but failed to show "out-of-pocket expenses").

[315] *Id.* at 979 ("Nowhere does the legislative history intimate that there was any congressional concern whatsoever regarding making the Government liable for proven damages in excess of out-of-pocket losses.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

The division between federal circuit courts continued in the 1990s. The Sixth Circuit joined the Eleventh Circuit,[316] while the Third Circuit joined the Fifth Circuit.[317] In the 2000s, however, the balance tipped toward the tort law theory of the invasion of privacy when the First and Fourth Circuits joined the Eleventh Circuit in *Orekoya v. Mooney* and *Doe v. Chao*.[318] More decisively, the United States Supreme Court ended the debate officially by affirming *Doe v. Chao* in 2004.[319]

In *Doe v. Chao*, plaintiff Buck Doe, in an action against the Secretary of Labor, alleged improper disclosure of his SSN.[320] Doe filed for black lung benefits with the Office of Workers' Compensation Programs in the Department of Labor, which required him to submit his SSN.[321] However, the Department not only used the SSN to identify claimants, but also sent the number to groups of claimants, their employers, and lawyers involved in their cases.[322] The government conceded that disclosing Doe's SSN violated the Privacy Act.[323] The question for the Court was whether Doe could claim statutory recovery under subsection (g)(4).[324] Justice David Souter, writing for the majority, endorsed the government's claim that "the minimum guarantee goes only to victims who prove some actual damages."[325] Justice Souter applied a "straightforward textual analysis" on the text of subsection (g)(4), and inferred that "[w]hen the statute gets to the point of guaranteeing the $1,000 minimum, it not only has confined any eligibility to victims of adverse effects caused by intentional or willful actions, but has provided expressly for liability to such victims for 'actual damages sustained.'"[326] In reaching his position, Justice Souter relied on a traditional tort theory and referred to it repeatedly:

---

[316] *See* DiMura v. FBI, 823 F. Supp. 45 (D. Mass. 1993); Hudson v. Reno, 130 F.3d 1193, 1207 (6th Cir. 1997).

[317] *See* Quinn v. Stone, 978 F.2d 126, 135–36 (3d Cir. 1992).

[318] Orekoya v. Mooney, 330 F.3d 1 (1st Cir. 2003); Doe v. Chao, 306 F.3d 170 (4th Cir. 2002).

[319] 540 U.S. 614, 616 (2004).

[320] *Id.* at 617.

[321] *Id.* at 616–17.

[322] *Id.* at 617.

[323] *Id.*

[324] *Id.*

[325] *Id.* at 620.

[326] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

> [T]he *traditional* understanding [is] that *tort* recovery requires not only wrongful act plus causation reaching to the plaintiff, but proof of some harm for which damages can reasonably be assessed.[327]
>
> . . . .
>
> [T]he reference in § 552a(g)(1)(D) to "adverse effect" acts as a term of art identifying a potential plaintiff who satisfies the *injury-in-fact* and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue.[328]

In her dissenting opinion, Justice Ginsburg stated:

> Privacy Act violations commonly cause fear, anxiety, or other emotional distress—in the Act's parlance, "adverse effects." Harm of this character must, of course, be proved genuine. In cases like Doe's, emotional distress is generally the only harm the claimant suffers, *e.g.*, the identity theft apprehended never materializes.[329]

Three decades after the passage of the Privacy Act, the Supreme Court's ruling in *Doe v. Chao* largely eliminated the "teeth" in the Privacy Act that Congress sought to provide in 1974.[330] This was achieved by imposing a traditional tort theory of privacy that Congress in 1974 had tried to reform.[331]

2. Section 7 of the Privacy Act

(a) Prohibition

Section 7(a)(1) prohibits denial of welfare benefits for failure to submit SSNs.[332] This is a narrowed-down version of Section 203 of Senate Bill 3418 initially

---

[327] *Id.* at 621 (emphasis added).

[328] *Id.* at 624 (emphasis added).

[329] *Id.* at 634 (Ginsburg, J., dissenting).

[330] Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 98 (2005).

[331] *Id.* at 96.

[332] Section 7(a)(1) of the Privacy Act of 1974 provides: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(1), 88 Stat. 1896, 1909 (1974).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

introduced in May 1974.[333] However, out of concerns for the probable costs and effects of such a broad prohibition, the Senate Committee decided to strike it out by a vote of eight to one in September 1974.[334] Senator Barry Goldwater introduced Amendment Number 1914 on November 21, 1974.[335] However, the October 1974 version of House Bill 16373 contained a narrower clause that is close to Section 7(a)(1).[336]

There are few cases showing straight applications of Section 7(a)(1). The first such case was a ruling by the United States District Court for the District of Columbia in *Wolman v. United States of America, Selective Service System*.[337] In July 1980, the Selective Service System reinstituted a program of military draft registration, which required each registrant to supply his SSN in addition to other information.[338] The United States District Court for the District of Columbia found that the program did not have legal authority to require SSNs and was thus in violation of Section 7 of the Privacy Act of 1974.[339] The court granted injunctive relief, enjoining the SSN requirement.[340] Still, Section 7 was dormant, so much so that in 2003, Judge Julie E. Carnes, sitting on the bench of the United States District Court for the Northern

---

[333] Section 203 of Senate Bill 3418 provides:

> It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program established under Title II of the Social Security Act) in whole or in part because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by law.

S. 3418, 93d Cong. § 203 (1974), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 247, at 23–24.

[334] S. REP. NO. 93-1183, at 28 (1974), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 247, at 181.

[335] SOURCE BOOK ON PRIVACY, *supra* note 247, at 763, 804 (proposing significant limitations on circumstances where government agencies could lawfully require SSNs).

[336] H. REP. NO. 93-1416 § 307(a) (Oct. 2, 1974), *in* SOURCE BOOK ON PRIVACY, *supra* note 247, at 373.

[337] 501 F. Supp. 310, 311 (D.D.C. 1980).

[338] Selective Service Regulations: Administration of Regulation, 45 Fed. Reg. 48130, 48131 (July 18, 1980) (codified at 32 C.F.R. pt. 1615.4(a)).

[339] *Wolman*, 501 F. Supp. at 311.

[340] *Id.* at 312.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

District of Georgia, came to the conclusion that Section 7 had become a "dead letter."[341] On appeal, the Eleventh Circuit reversed that ruling and revived the Section 7 in federal courts.[342]

(b) Collection: Exceptions

Section 7(a)(2) created two exceptions to the general rule on data collection. Subsection (A) allowed disclosure of the SSN if such disclosure is required by federal statutes; subsection (B) grandfathered disclosures required by statute or regulation prior to January 1, 1975.[343]

Shortly after the Privacy Act took effect, a number of cases relating to Aid to Families with Dependent Children ("AFDC") programs were brought to the courts across the country. Parents who were denied AFDC benefits for having refused to provide their children's SSNs contended that the denial violated Section 7 of the Privacy Act.[344] Shortly after the Privacy Act of 1974, Congress amended the Social

---

[341] Schwier v. Cox, 340 F.3d 1284, 1288 (11th Cir. 2003) (quoting Schwier v. Cox, No. 00-02820-CV-JEC-1 (N.D. Ga.)).

[342] *Id.* at 1286; *see also* Ky. Rest. Concepts, Inc. v. City of Louisville, 209 F. Supp. 2d 672, 676–77, 686–87 (W.D. Ky. 2002) (city ordinance that would deny a license for failure to submit SSN violated the Privacy Act); Stollenwerk v. Miller, No. Civ.A. 04–5510, 2006 WL 463393, at *1 (E.D. Pa. Feb. 24, 2006) (SSN not required for purchase of a gun or for license); Ingerman v. Del. River Port Auth., 630 F. Supp. 2d 426, 428, 443, 445 (D.N.J. 2009) (SSN not required for E-ZPass Senior Citizen Program enrollment). Despite this change, federal circuits are still split on the question of whether state governments are covered by the Privacy Act. *See* Dittman v. California, 191 F.3d 1020, 1026–1027 (9th Cir. 1999) (ruling that Section 7 did not provide a cause of action against state requirement for acupuncturist to provide SSN upon applying for license renewal).

[343] Section 7(a)(2) provides:

> [T]he provisions of paragraph (1) of this subsection shall not apply with respect to—
> (A) any disclosure which is required by Federal statute, or
> (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(2), 88 Stat. 1896, 1909 (1974).

[344] *See, e.g.*, Chambers v. Klein, 419 F. Supp. 569, 571–73 (D.N.J. 1976), *aff'd mem.*, 564 F.2d 89 (3d Cir. 1977); Green v. Philbrook, 576 F.2d 440, 441, 445–46 (2d Cir. 1978), *rev'g* 427 F. Supp. 834 (D. Vt. 1977); Arthur v. Wash. State Dep't of Soc. & Health Servs., 576 P.2d 921, 923–25 (Wash. Ct. App. 1978);

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Security Act by enacting Public Law 93-647,[345] which required a state AFDC program to collect an SSN from each applicant in order to be eligible for AFDC benefits.[346] In *Chambers v. Klein*, for example, the district court ruled that "the disclosure of the social security numbers under the state and federal regulations comes within the exception set forth in Section 7(a)(2)(A) of the Privacy Act."[347]

In October 1976, Congress again amended the Social Security Act by enacting Public Law 94-455, known as the Tax Reform Act of 1976.[348] The amendment explicitly allowed states to utilize SSNs to establish identification.[349] In *Doe v.*

Greater Cleveland Welfare Rts. Org. v. Bauer, 462 F. Supp. 1313, 1314–15 (N.D. Ohio 1978) (class-action suit with a named plaintiff); McElrath v. Califano, 615 F.2d 434, 435–37 (7th Cir. 1980); Doe v. Sharp, 491 F. Supp. 346, 347–48 (D. Mass. 1980).

[345] Social Services Amendments of 1974, Pub. L. No. 93-647, 88 Stat. 2337 (1975).

[346] Section 6305(c)(5) of the Social Services Amendments of 1974 provides in relevant part:

> that, as a condition of eligibility under the plan, each applicant for or recipient of aid shall furnish to the State agency his social security account number . . . and (B) that such State agency shall utilize such account numbers, in addition to any other means of identification it may determine to employ in the administration of such plan . . . .

Id. at 2359 (codified as amended at 42 U.S.C. § 602(a)(25)).

[347] 419 F. Supp. at 580.

[348] Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (codified as amended at 42 U.S.C. § 405).

[349] Section 1211(b) of the Tax Reform Act of 1976 provides in relevant part:

> It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the Secretary for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number (or numbers, if he has more than one such number) issued to him by the Secretary.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Sharp, the United States District Court for the District of Massachusetts considered that by enacting this amendment, Congress "has specifically overruled the limitations imposed by [Section] 7(a)."[350]

Another law that made an impact was Public Law 97-86,[351] which was recognized by the court in *Wolman v. United States*.[352] As mentioned earlier, in the 1980 *Wolman* case, the district court issued an injunction against a military draft registration program requiring disclosure of SSNs.[353] While the case was on appeal, Congress enacted Public Law 97-86.[354] Having been satisfied that Congress had cured the problem by legislative authorization, the district court, in 1982, dismissed further litigation on the matter.[355] In 2021, the Eleventh Circuit addressed a passport renewal denied for refusing to provide an SSN under Public Law 114-94, ruling that the law cured any violation of the Privacy Act.[356]

Id. at 1711–12 (codified as amended at 42 U.S.C. § 405(c)(2)(C)(i)). For a commentary on Section 1211 of the Tax Reform Act of 1976, see Stephen Mayer, *Privacy and the Social Security Number: Section 1211 of the Tax Reform Act of 1976*, 6 RUTGERS J. COMPUTS. & L. 221 (1978).

[350] 491 F. Supp. 346, 349 (D. Mass. 1980); *see also* Kaufmann v. Dep't of Pub. Welfare, 778 A.2d 795, 796, 798–99 (Pa. Commw. Ct. 2001) (food stamp recipient lost benefits after refusing to disclose SSN); North Carolina *ex rel.* Kasler v. Howard, 323 F. Supp. 2d 675, 678–79 (W.D.N.C. 2003) (holding that the Tax Reform Act of 1976 provided the authority for the state's Department of Motor Vehicle to require a SSN for the application of a driver's license); Peterson v. City of Detroit, 76 F. App'x 601, 602 (6th Cir. 2003) (application for a taxicab license lawfully turned down for refusal to disclose a SSN); Greidinger v. Almand, 30 F. Supp. 3d 413, 414–15, 420–21, 424–26 (D. Md. 2014) (attorney's license renewal lawfully denied for refusing to disclose a SSN).

[351] Department of Defense Authorization Act, 1982, Pub. L. No. 97-86, 95 Stat. 1099 (1981). Section 916(a)(2) of the Act amended the Military Selective Service Act by adding the following: "(b) Regulations prescribed pursuant to subsection (a) may require that persons presenting themselves for and submitting to registration under this section provide, as part of such registration, such identifying information (including date of birth, address, and social security account number) as such regulations may prescribe." *Id.* at 1129.

[352] 542 F. Supp. 84, 84 (D.D.C. 1982).

[353] Wolman v. U.S. Selective Serv. Sys., 501 F. Supp. 310, 312 (D.D.C. 1980).

[354] Department of Defense Authorization Act § 916(a)(2).

[355] *Wolman*, 542 F. Supp. at 84–86.

[356] Whitfield v. U.S. Sec'y of State, 853 F. App'x 327, 328, 329, 331 (11th Cir. 2021) (per curiam) (holding that denying a passport renewal application for refusing to provide a SSN was legal). The FAST Act provides in relevant part:

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Subsection (B) of the Privacy Act grandfathered disclosures required by statute or regulation prior to January 1, 1975.[357] In *Brookens v. United States*, the State Department denied travel advances to those employees who refused to disclose their SSNs, relying on Executive Order 9397 issued by the President in 1943.[358] The DC Circuit ruled that Executive Order 9397 "is within the meaning of a regulation" under Section 7(a)(2)(B).[359] In its 1977 study, the Privacy Protection Study Commission noted that Executive Order 9397 "has been cited by some Federal agencies as the legal authority";[360] however, the Commission concluded, "to the extent that Federal agencies interpret E.O. 9397 as sufficient authority to establish requirements for collection of the SSN, the intent of Section 7 is undermined."[361] The Commission recommended that federal agencies do not rely on Executive Order 9397 after

> [U]pon receiving an application for a passport from an individual that either—(i) does not include the social security account number issued to that individual, or (ii) includes an incorrect or invalid social security number willfully, intentionally, negligently, or recklessly provided by such individual, the Secretary of State is authorized to deny such application and is authorized to not issue a passport to the individual.

Id. at 329; FAST Act, Pub. L. No. 114-94, § 7345(f)(1)(A), 129 Stat. 1312, 1732–33 (2015) (codified as amended at 22 U.S.C. § 2714a(f)(1)(A)).

[357] Section 7(a)(2) provides:

> [T]he provisions of paragraph (1) of this subsection shall not apply with respect to . . . (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(2), 88 Stat. 1896, 1909 (1974).

[358] 627 F.2d 494, 497–98 (D.C. Cir. 1980).

[359] *Id.* at 498.

[360] PRIV. PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION 616 (1977).

[361] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

January 1, 1977.[362] However, the *Brookens* ruling in 1980 suggests that the DC Circuit totally ignored the recommendation.[363]

(c) Use of SSNs

Section 7(b) of the Privacy Act of 1974 requires a government agency requesting an SSN to inform the data subjects whether the request is mandatory or not, as well as the use for the SSN.[364]

In *Chambers v. Klein*, plaintiffs complained that at no time were they told what uses would be made of the SSNs by New Jersey welfare officials.[365] New Jersey argued that the State was at the time making no use of the SSNs; it collected the numbers only because federal statutes and regulations required so.[366] Plaintiffs then "urge[d] that the State should not demand [SSNs] as a prerequisite to AFDC assistance unless it plan[ned] to utilize the numbers."[367] The district court rejected the argument that the social security numbers should not have been demanded from plaintiffs unless a use of them was contemplated.[368] The court concluded that plaintiffs' rights under Section 7(b) of the Privacy Act have not been violated.[369] Sensing a need for justification, the court stated: "In that regard, I place particular weight upon the fact that [federal regulations] were issued pursuant to the authorization of a federal statute requiring the disclosure of social security numbers."[370] Here, the court clearly assumed exceptions under Section 7(a) would exonerate the obligation to inform of the use of SSNs under Section 7(b). The court conflated Sections 7(a) with 7(b) without looking into the legislative history.

---

[362] *Id.* at 616–17.

[363] *Brookens*, 627 F.2d at 498–99.

[364] Section 7(b) provides: "Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." Privacy Act of 1974, Pub. L. No. 93-579, § 7(b), 88 Stat. 1896, 1909 (1974).

[365] 419 F. Supp. 569, 579 (D.N.J. 1976), *aff'd mem.*, 564 F.2d 89 (3d Cir. 1977).

[366] *Id.*

[367] *Id.*

[368] *Id.* at 580.

[369] *Id.*

[370] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

In *McElrath v. Califano*, Doris McElrath, the mother of two minor children from Illinois, argued that the AFDC statute violated Section 7(b) by requiring disclosure of SSNs without informing her of the purpose for which the numbers were being required and by denying benefits for failure to disclose the SSNs.[371] The district court considered the failure to inform a "mere technical violation which would be rectified" by a notice to be sent out by the Illinois government.[372] On appeal, McElrath raised the issue again, but the Seventh Circuit ignored it in affirming the lower court's decision.[373]

In *Greater Cleveland Welfare Rights Organization v. Bauer*, families with dependent children challenged a request by the welfare department in Ohio for SSNs of recipients, which it then used in a match program without prior permission, creating a violation of Section 7 of the Privacy Act of 1974.[374] The question focused on whether Section 7(b) conferred plaintiffs with a private cause of action for the alleged violation.[375] The district court ruled that "Section 7(b) does create an especial right in plaintiffs and the class they represent."[376] According to the court:

> It is clear that in enacting Section 7(b), Congress intended to insure that individuals in the position of plaintiffs and their class could make an informed decision on whether to comply with a request for their social security numbers and to protect such individuals from unauthorized uses of said numbers.[377]

The court found the Ohio AFDC program to be in violation of Section 7(b).[378] However, the *Bauer* ruling is an exception to court rulings during the first decade after the Privacy Act of 1974 was enacted.[379]

---

[371] 615 F.2d 434, 437 (7th Cir. 1980).

[372] *Id.* at 438.

[373] *Id.* at 438, 441.

[374] 462 F. Supp. 1313, 1313–14 (N.D. Ohio 1978).

[375] *Id.* at 1319.

[376] *Id.*

[377] *Id.*

[378] *Id.* at 1321.

[379] *Bauer* was followed by Yeager v. Hackensack Water Co., 615 F. Supp. 1087, 1091 (D.N.J. 1985).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

B. Disclosure of the SSN and the Constitution

Privacy advocates in the late 1960s and early 1970s were inspired by several rulings from the Supreme Court—*Griswold v. Connecticut*,[380] *Katz v. United States*,[381] and *Roe v. Wade*.[382] However, there is a clear contrast on the Court's view on privacy before and after the enactment of the Privacy Act of 1974.[383] The Court had decisively turned against its privacy jurisprudence in two decisions that fundamentally changed the path of privacy protection under the Constitution: *Paul v. Davis* and *McElrath v. Califano*.[384]

1. The Scope of Privacy

In *Paul v. Davis*, then Associate Justice William H. Rehnquist declared that the "right of privacy" described in the past cases were "substantive aspects of the Fourteenth Amendment" that were typically "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education."[385] More specific language came from the majority opinion of *Roe v. Wade*.[386] However, the *Roe* Court made the statement in 1973 trying to build on an emerging jurisprudence on the principle of privacy, while in 1976, Justice Rehnquist was trying to impose a boundary on privacy to prevent it from expanding to other areas, such as

---

[380] 381 U.S. 479 (1965).

[381] 389 U.S. 347 (1967).

[382] 410 U.S. 113 (1973), *overruled by* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

[383] *Compare id.* at 154 (demonstrating an expansive view of the application of the right to privacy), *with* Paul v. Davis, 424 U.S. 693, 713 (1976) (demonstrating a narrow view of the application of the right to privacy).

[384] *See Davis*, 424 U.S. at 713; McElrath v. Califano, 615 F.2d 434, 441 (7th Cir. 1980).

[385] *Davis*, 424 U.S. at 713.

[386] Where the Supreme Court tracked earlier rulings on privacy:

> These decisions make it clear that only personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty,' are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage, procreation, contraception, family relationships, and child rearing and education.

Roe, 410 U.S. at 152–53 (citations omitted).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

names, addresses, and other personally identifying information.[387] While he would do more to roll back the Warren Court's progress on privacy later in his capacity as Chief Justice, Rehnquist was engaged in a battle against privacy rights before and after the Privacy Act.[388]

Rehnquist had some close contact with Barry Goldwater while serving as a legal adviser for Goldwater's presidential campaign in 1964.[389] In 1969, he was appointed Assistant Attorney General.[390] In that capacity, Rehnquist testified before Senator Ervin's subcommittee in March 1971, insisting that government information gathering or surveillance did not violate citizens' constitutional rights.[391] Rehnquist told Senator Ervin's Subcommittee that

[387] *Compare id.* at 154 (demonstrating an expansive view of the application of the right to privacy), *with Davis*, 424 U.S. at 713 (demonstrating a narrow view of the application of the right to privacy).

[388] *See, e.g.*, SUE DAVIS, JUSTICE REHNQUIST AND THE CONSTITUTION 21, 23, 27 (1989); Melissa Arbus, Note, *A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era*, 89 VA. L. REV. 1729, 1733 (2003); Scott P. Johnson & Robert M. Alexander, *The Rehnquist Court and the Devolution of the Right to Privacy*, 105 W. VA. L. REV. 621, 649–50 (2003); Mark A. Racanelli, Note, *Reversals: Privacy and the Rehnquist Court*, 81 GEO. L.J. 443, 446 (1992); Laurence A. Benner, *Diminishing Expectations of Privacy in the Rehnquist Court*, 22 J. MARSHALL L. REV. 825, 826 (1989).

[389] JOHN A. JENKINS, THE PARTISAN: THE LIFE OF WILLIAM REHNQUIST 72–73 (2012).

[390] *Federal Data Banks Hearings*, *supra* note 96, at 849 (statement of William H. Rehnquist, Assistant Att'y Gen., Department of Justice).

[391] At the hearing on March 17, 1971, Senator Ervin asked Rehnquist: "Army intelligence agents, pretending to be photographers, were present at many rallies, took pictures of people, and then made inquiries to identify these people and made dossiers of them. Do you not think that is a interference of constitutional rights?" *Id.* at 861–62. Rehnquist replied:

> I think, from my reading of the cases, that the time at which the courts would say there has been an interference with an individual's constitutional rights in that area is where the Government seeks by some sort of legal sanction either to compel divulgence of information or to put the information it has gathered without compulsion to some use such as a criminal prosecution or a civil action against the individual.
>
> I don't think the gathering by itself, so long as it is a public activity, is of constitutional stature.

Id. at 862.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

> the Department [of Justice] will vigorously oppose any legislation which, whether by opening the door to unnecessary and unmanageable judicial supervision of such activities or otherwise, would effectively impair this extraordinarily important function of the Federal Government.[392]

It sounded like a threat, and an intimidating one. In October 1971, President Richard Nixon nominated Rehnquist to the United States Supreme Court.[393] As Associate Justice on the nation's highest court, Rehnquist continued his battle against an expanding right to privacy.[394] In his dissenting opinion in *Roe v. Wade* in 1973, Rehnquist equated the *Roe* majority's view on privacy with the *Lochner* ruling.[395] In September 1974, three months before Congress passed the Privacy Act, he delivered public lectures arguing against "claims to increased privacy."[396]

In 1976, the *Paul v. Davis* case provided a perfect opportunity for Justice Rehnquist to codify his views on privacy.[397] In this case, Davis was arrested in a Louisville, Kentucky store by a private security officer for shoplifting, and he pleaded not guilty to the charge.[398] While the charge was outstanding in late 1972, Paul, the chief of police of Louisville, printed and distributed a flyer to 800 merchants which contained names and photographs of "active shoplifters."[399] That list included Davis.[400] Davis filed suit alleging deprivation of his "liberty" and "property" rights under the Due Process Clause of the Fourteenth Amendment, as

---

[392] *Id.* at 603–04.

[393] *Nixon and the Supreme Court*, RICHARD NIXON PRESIDENTIAL LIBR. & MUSEUM (Sept. 22, 2021), https://www.nixonlibrary.gov/news/nixon-and-supreme-court [https://perma.cc/A3SU-RPKE].

[394] *See* Roe v. Wade, 410 U.S. 113, 171 (1973) (Rehnquist, J., dissenting), *overruled by* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

[395] *Id.* at 174 ("While the Court's opinion quotes from the dissent of Mr. Justice Holmes in *Lochner v. New York* . . . the result it reaches is more closely attuned to the majority opinion of Mr. Justice Peckham in that case.").

[396] William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, 23 U. KAN. L. REV. 1, 21 (1974) (detailing lectures delivered at the University of Kansas School of Law on September 26 and 27, 1974).

[397] *See* 424 U.S. 693, 713 (1976).

[398] *Id.* at 694–96.

[399] *Id.* at 694–95.

[400] *Id.* at 695.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

well as his constitutional right to privacy.[401] Writing for a conservative majority, Rehnquist made the statement, quoted earlier, to prevent the further expansion of earlier privacy rights precedents: "None of our substantive privacy decisions hold this or anything like this, and we decline to enlarge them in this manner."[402] *Paul v. Davis* was a setback in privacy litigation in the broadest sense;[403] however, the case itself was not about SSNs. Thus, it is important to note that Justice Rehnquist was not alone in the judicial reaction to the Privacy Act. In *McElrath v. Califano*, the Seventh Circuit came to the same conclusion without citing *Paul v. Davis*.[404] The Seventh Circuit here followed the same approach as Rehnquist—citing *Roe*.[405] It derived the same *Paul v. Davis* principle: "The constitutional guarantee of the right to privacy embodies only those personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty.'"[406] Then the court came to its own assessment, as if it were not apparent:

> Accordingly, we regard the decision of Mrs. McElrath whether or not to obtain social security account numbers for her two minor children in order to receive welfare benefits as involving neither a fundamental right nor a right implicit in the concept of ordered liberty.[407]

McElrath became the first major circuit court ruling to exclude any role of the Constitution in protecting privacy. In 1982, the federal district court in Delaware, citing both *Paul v. Davis* and *McElrath*, observed that federal courts "have held, and this Court concurs in that view, that mandatory disclosure of one's social security number does not so threaten the sanctity of individual privacy as to require

[401] *Id.* at 696–97.

[402] *Id.* at 713. *See* Mark Tushnet, *The Constitutional Right to One's Good Name: An Examination of the Scholarship of Mr. Justice Rehnquist*, 64 KY. L.J. 753, 753–54 (1976).

[403] Barbara E. Armacost, *Race and Reputation: The Real Legacy of* Paul v. Davis, 85 VA. L. REV. 569, 584 (1999); Randolph J. Haines, Note, *Reputation, Stigma and Section 1983: The Lessons of* Paul v. Davis, 30 STAN. L. REV. 191, 207–08 n.101 (1977).

[404] *See* 615 F.2d 434, 441 (7th Cir. 1980).

[405] *Id.*

[406] *Id.* (quoting Roe v. Wade, 410 U.S. 113, 152 (1973)).

[407] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

constitutional protection."[408] Within the first decade of the Privacy Act, it was settled law that the Constitution had little role to play in the privacy of SSNs.[409]

2. SSNs and the First Amendment

The First Amendment issue has been raised in the context of mandatory disclosure of SSNs. In the Aid to Families with Dependent Children ("AFDC") program,[410] the issue eventually came to the United States Supreme Court in *Bowen v. Roy*.[411] In this case, plaintiff Roy refused to use an SSN for his three-year-old daughter, Little Bird of the Snow, on the ground that doing so would be contrary to their native Abenaki Indian religious beliefs.[412] He also believed that use of SSNs had the effect of "robbing the spirit of man."[413] After their AFDC benefits were terminated, Roy challenged the welfare agency's decision, alleging that the First Amendment entitled them to an exemption from the SSN requirement.[414]

Chief Justice Warren Burger, writing for the majority, rejected the claims based on the Free Exercise Clause.[415] According to Chief Justice Burger, "[t]he requirement that applicants provide a social security number is facially neutral and applies to all applicants for the benefits involved."[416] Commentators have noted the shift in free exercise jurisprudence.[417] It is perhaps puzzling that the ideologically conservative Burger Court adopted a constitutional standard in favor of the welfare

---

[408] Doyle v. Wilson, 529 F. Supp. 1343, 1348 (D. Del. 1982).

[409] Cassano v. Carb, 436 F.3d 74, 75 (2d Cir. 2006) (per curiam); Spurlock v. Ashley Cnty., 281 F. App'x 628, 629 (8th Cir. 2008); North Carolina *ex rel.* Kasler v. Howard, 323 F. Supp. 2d 675, 679 (W.D.N.C. 2003) ("In fact, 'the contention that disclosure of one's SS account number violates the right to privacy has been consistently rejected in other related contexts.'") (citations omitted).

[410] Roy v. Cohen, 590 F. Supp. 600 (M.D. Pa. 1984), *vacated sub nom.* Bowen v. Roy, 476 U.S. 693 (1986).

[411] 476 U.S. at 695.

[412] *Id.*

[413] *Id.* at 696 (internal quotations omitted).

[414] *Id.* at 695.

[415] *Id.* at 699.

[416] *Id.* at 708.

[417] Paul E. McGreal, *The Making of the Supreme Court's Free Exercise Clause Jurisprudence: Lessons from the Blackmun and Powell Papers in* Bowen v. Roy, 34 S. ILL. U. L.J. 469, 469 (2010); Marc J. Bloostein, *Core Periphery Dichotomy in First Amendment Free Exercise Clause Doctrine in* Goldman v. Weinberger, Bowen v. Roy, *and* O'Lone v. Estate of Shabazz, 72 CORNELL L. REV. 827, 827 (1987).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

state.[418] What is more astonishing is the fact that twelve years after the passage of the Privacy Act, Chief Justice Burger spoke of the use of SSNs for matching approvingly:

> Social security numbers are unique numerical identifiers and are used pervasively in these programs. The numbers are used, for example, to keep track of persons no longer entitled to receive food stamps because of past fraud or abuses of the program. Moreover, the existence of this unique numerical identifier creates opportunities for ferreting out fraudulent applications through computer "matching" techniques.[419]

The dissenting Justices—Justice Sandra Day O'Connor, joined by Justices William Brennan and Thurgood Marshall, who dissented in part—challenged the majority's rationale for its lack of guidance to the welfare state,[420] and rightly warned that "[t]he rise of the welfare state was not the fall of the Free Exercise Clause."[421] However, they had nothing to say about the privacy issue and the matching techniques. Three months after the *Bowen* ruling, Senator Cohen introduced Senate Bill 2756, the Computer Matching and Privacy Act.[422]

IV. THE PRIVACY REVOLUTION ABROAD

The fate of the Privacy Act of 1974 and the lack of a constitutional recognition of data privacy in the United States suggest a failure in its legal response to the

[418] *Bowen*, 476 U.S. at 699 ("The Free Exercise Clause simply cannot be understood to require the Government to conduct its own internal affairs in ways that comport with the religious beliefs of particular citizens.").

[419] *Id.* at 710.

[420] *Id.* at 727 (O'Connor, J., joined by Brennan & Marshall, JJ., concurring in part and dissenting in part) ("[The Chief Justice] would uphold any facially neutral and uniformly applicable governmental requirement if the Government shows its rule to be 'a reasonable means of promoting a legitimate public interest.'").

[421] *Id.* at 732 (O'Connor, J., concurring in part and dissenting in part).

[422] *Computer Matching and Privacy Protection Act of 1986: Hearing on S. 2756 Before the Subcomm. on Oversight of Gov't Mgmt. of the S. Comm. on Governmental Affs.*, 99th Cong. 1–2 (1986). Concerns about computer matching were raised earlier. *See* John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 991–92 (1984); Kenneth James Langan, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J.L. & SOC. PROBS. 143, 143 (1979).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

computer.[423] Outside the United States, however, the privacy revolution continued.[424] Over time, the revolution's central thesis of empowering individuals and the fundamental principles enabling them to control data evolved into a constitutional doctrine called "informational self-determination."[425] It started in 1983 in a ruling of the German *Bundesverfassungsgericht* (Federal Constitutional Court).[426] The doctrine expanded and went beyond Europe—it was embraced by the Taiwan constitutional court *Sifayuan Dafaguan Huiyi* (Council of Grand Justices) in 2004 and the South Korean *Heonbeop Jaepanso* (Constitutional Court) in 2005.[427] In August 2017, the doctrine was enthusiastically adopted by the Indian Supreme Court.[428] It was embraced by privacy advocates in Japan in their ongoing constitutional battle against the "My Number" system.[429]

A. The European Union

As this Article previously discussed, by the late 1970s, many European countries had their first generation of data protection laws.[430] They began to coordinate legal norms around Europe.[431] The Council of Europe drafted the first international convention in January 1980.[432] After one year of deliberation, it became official in January 1981, as the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the "Personal Data

[423] Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1322, 1346 (1992).

[424] *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 BVERFGE 1, para. 1–2 (Ger.).

[425] *Id.* at 14, para. 146.

[426] *Id.*

[427] Interpretation of the Judicial Yuan Case No. 585, 2004 SHIZI para. 1 (Constitutional Ct. Dec. 15, 2004) (Taiwan), https://perma.cc/FL2M-YDW8; ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 358–59 (Ronald Deibert, Rafal Rohozinski, John Palfrey & Jonathan Zittrain eds., 2012) [hereinafter ACCESS CONTESTED].

[428] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

[429] Kazuhiro Toyama, *Japan Top Court Rules 'My Number' ID System Constitutional Amid Privacy Violation Claims*, MAINICHI (Mar. 10, 2023), https://mainichi.jp/english/articles/20230310/p2a/00m/0na/019000c [https://perma.cc/ADQ5-59PQ].

[430] *See supra* Section II.D.

[431] *See id.*

[432] Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 10, 1980, 19 I.L.M. 282, 284 *reprinted in* DOCUMENTS ON DATA PROTECTION (1980).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Convention").[433] The OECD was primarily interested in transborder data flow, given growing tension over the disparity in law that led to the "data war" between Europe and the United States.[434] In December 1979, the OECD adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines").[435] Both the Convention and the OECD Guidelines reflect the fundamental principles behind the Privacy Act of 1974 in the United States.

However, the legal response to the computer in Europe did not stop there. In the early 1980s, European governments continued to update their data protection laws.[436] The most consequential development was in 1983, when the German Constitutional Court decided the *Census Act Case*.[437] The court ruled that "[t]he value and dignity of the person, acting in free self-determination as a member of a free society, are at the centre of the Basic Law."[438] The court noted that earlier cases had implied that "based on the notion of self-determination, the general right of personality confers upon the individual the authority to, in principle, decide themselves whether and to what extent to disclose aspects of their personal life."[439]

---

[433] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 108 E.T.S. 1 [hereinafter Personal Data Convention].

[434] *The World Data War*, NEW SCI., Sept. 3, 1981, at 604; A.C. Evans, *European Data Protection Law*, 29 AM. J. COMPAR. L. 571, 581–82 (1981); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1318–19 (2000).

[435] Draft Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Dec. 12, 1979, 19 I.L.M. 318, 318, *reprinted in* DOCUMENTS ON DATA PROTECTION (1980).

[436] Colin Mellors & David Pollitt, *Legislating for Privacy: Data Protection in Western Europe*, 37 PARLIAMENTARY AFFS. 199, 199 (1984) (noting that Austria, Demark, France, Iceland, Luxembourg, Norway, Sweden, and West Germany had their data protection legislation in force, while Belgium, Finland, Italy, Netherlands, Portugal and Switzerland were in the process of doing so).

[437] 65 BVERFGE 1 (Ger.). For commentary on the case, see Eckhart K. Gouras, Note, *The Reform of West German Data Protection Law as a Necessary Correlate to Improving Domestic Security*, 24 COLUM. J. TRANSNAT'L L. 597, 608–12 (1986); Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMPAR. L. 675, 687–92 (1989); DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 323–25 (2d ed. 1997); Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 1997 UTAH L. REV. 963, 1000–07 (1997).

[438] 65 BVERFGE 1, 14, para. 144 (Ger.). "Basic Law" refers to the Constitution of the Federal Republic of Germany. *See Constitution of the Federal Republic of Germany*, FED. MINISTRY OF THE INTERIOR & CMTY., https://www.bmi.bund.de/EN/topics/constitution/constitutional-issues/constitutional-issues.html [https://perma.cc/U7LQ-GNRZ] (last visited, Sept. 9, 2024).

[439] 65 BVERFGE 1, 14, para. 144 (Ger.).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

The court then applied this principle to the digital world: "Given the present and future realities of automatic data processing, this authority conferred upon the individual merits special protection."[440] In conclusion, the court declared:

> In the context of modern data processing, the free development of one's personality therefore requires that the individual be protected against the unlimited collection, storage, use and sharing of their personal data. Consequently, the fundamental right of Art. 2(1) in conjunction with Art. 1(1) of the Basic Law encompasses such protection. In this regard, the fundamental right confers upon the individual the authority to, in principle, decide themselves on the disclosure and use of their personal data.[441]

The ruling in the *Census Act Case*, made in the midst of intensive German domestic politics,[442] is a powerful recognition that, in the computer age, the individual can have certain controls over the data about herself even beyond the reach of the bureaucrats. It is a constitutionally protected fundamental right.

B. The Commonwealth Countries

The commonwealth countries faced more delays in enacting their first-generation data protection laws. In Canada, the first federal public sector privacy legal framework was enacted in July 1977 in Part IV of the Canadian Human Rights Act.[443] Canada followed European nations in establishing an Office of the Privacy Commissioner,[444] who had the power to receive complaints from the general

[440] *Id.* at para. 145.

[441] *Id.* at 15, para. 147.

[442] *See, e.g.*, William P. Butz, *Data Confidentiality and Public Perceptions: The Case of the European Censuses*, *in* AM. STAT. ASS'N, PROCEEDINGS OF THE SURVEY RESEARCH METHODS SECTION 90–97 (1985), http://www.asasrms.org/Proceedings/papers/1985_016.pdf [https://perma.cc/55HL-TKWU]; THE POLITICS OF NUMBERS 417 (Paul Starr & William Alonso eds., 1987); LARRY FROHMAN, THE POLITICS OF PERSONAL INFORMATION: SURVEILLANCE, PRIVACY, AND POWER IN WEST GERMANY 95 (2021); MAJID TEHRANIAN, TECHNOLOGIES OF POWER: INFORMATION MACHINES AND DEMOCRATIC PROSPECTS 124, 131 (1990).

[443] Canadian Human Rights Act, July 14, 1977, S.C. 1976–77, c 33, Part IV (Protection of Personal Information) (Can.).

[444] *Id.* c P-57.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

public,[445] conduct investigations and report its findings,[446] and make recommendations to Parliament.[447] The 1977 Act also prescribed the general rules of confidentiality[448] and rules on access and use of records,[449] but with broad exemptions for national security and law enforcement areas.[450] Five years later in 1982, a separate Privacy Act received royal assent and replaced the 1977 Act.[451] If the 1977 Act was a framework, the 1982 Privacy Act was a fully developed set of rules on data privacy.[452]

The United Kingdom faced more delays. In the early 1980s, international pressure was mounting. The OECD Guidelines were adopted in September 1980.[453] While they had no legal effect, the rapid increase in transborder data flow in banking and airline industries and the growth of international trade in computer hardware and services created pressure for data protection legislation as "widespread belief within the Department of Industry and elsewhere" developed that the UK data processing industry suffered due to the lack of legislation.[454] The UK signed the Personal Data

[445] *Id.* c P-58.

[446] *Id.* c P-31.

[447] *Id.* c P-60.

[448] *Id.* c P-50.

[449] *Id.* c P-52.

[450] *Id.* c P-54.

[451] Access to Information and Privacy Act, S.C. 1980, c 43, Scheds. I–II (Can.).

[452] For commentary on the Act, see Stephen J. Skelly, *Data Protection Legislation in Canada*, 3 Y.B.L. COMPUTS. & TECH. 79 (1987); Peter Gillis, *The Privacy Act: A Legislative History and Overview*, 1987 CAN. HUM. RTS. Y.B. 119 (1987); and T. Murray Rankin, *The New Access to Information and Privacy Act: A Critical Annotation*, 15 OTTAWA L. REV. 1 (1983).

[453] Org. for Econ. Coop. & Dev. [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL [https://perma.cc/2T5S-3DYL].

[454] Anne Crook, *Data Protection in the United Kingdom: Part 1*, 7 J. INF. SCI. 15, 18 (1983). Similarly, a scholar writing in 1984 noted:

> The primary purpose of the present Act is to avoid damage to our international trade which may contribute to result from countries' refusing to trade with the UK, for example Sweden, because of inadequate safeguards in respect of personal data.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Convention in Strasbourg in May 1981.[455] In April 1982, a proposal for privacy legislation was published.[456] On July 12, 1984, the Data Protection Act received the royal assent.[457] Australia passed its Privacy Act in 1988,[458] and New Zealand passed its own in 1993.[459]

Even with these data protection laws, there are still privacy issues not addressed. In the UK, the National Insurance number and the National Health Service number ("NHS") cover the entire population.[460] The 1978 Lindop Report, which devoted a chapter to universal personal identifiers ("UPI"),[461] noted that in the UK the National Insurance number was increasingly used as a UPI.[462] Drawing lessons from the U.S. experience, the Lindop Report recommended that a UPI should not be permitted.[463] After the Data Protection Act 1984 took effect, Eric Howe—the UK's first data protection registrar—observed increased interest in introducing

---

> We were one of the few remaining Western European countries not to have enacted data protection laws by the beginning of 1984.

David Price, *The Emergence of a UK Data Protection Law*, 1 Y.B.L. COMPUTS. & TECH. 131, 131–32 (1984). *See also* Priscilla M. Regan, *Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations*, 4 J. PUB. POL'Y 19, 35 (1984) ("It appears that legislative action may now be forthcoming, but the government's programmatic goal in seeking legislation is to protect British economic interests, not to protect personal privacy.").

[455] Personal Data Convention, *supra* note 433. The United Kingdom signed up for the Convention on May 14, 1981, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, May 16, 1983, 1496 U.N.T.S. 65, 88.

[456] HOME OFFICE, DATA PROTECTION: THE GOVERNMENT'S PROPOSALS FOR LEGISLATION, 1982, Cm. 8539 (UK).

[457] Data Protection Act 1984, c. 35 (U.K.); Nigel Savage & Chris Edwards, *The Legislative Control of Data Processing—The British Approach*, 6 COMPUT. L.J. 143, 143 (1985); Eric Howe, *The United Kingdom's Data Protection Act*, 8 GOV'T INFO. Q. 345, 345 (1991).

[458] *Privacy Act 1988* (Cth) (Austl.). For commentary, see Lee A. Bygrave, *The Privacy Act 1988 (Cth): A Study in the Protection of Privacy and the Protection of Political Power*, 19 FED. L. REV. 128 (1990).

[459] Privacy Act 1993 (N.Z.). For commentary, see John M. Howells, *The Privacy Act of 1993: A New Zealand Perspective*, 17 COMPAR. LAB. L.J. 107 (1995).

[460] JOSH CHANG, FELIX PEYSAKHOVICH, WEIMIN WANG & JIN ZHU, THE UK HEALTH CARE SYSTEM, http://assets.ce.columbia.edu/pdf/actu/actu-uk.pdf [https://perma.cc/2G7J-WPYR].

[461] HOME OFFICE, REPORT OF THE COMMITTEE ON DATA PROTECTION, 1978, Cm. 7341, at 260–64 (UK).

[462] *Id.* at 263.

[463] *Id.* at 264.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

national identity cards and national identity numbers and advised against such ideas.[464] In 1994, Howe again warned that National Insurance number and NHS number were becoming de facto personal identifiers.[465] Contrary to Howe's advice, more proposals to create a new national identification card emerged in the 1990s.[466] After September 11, 2001, these efforts reemerged, culminating in the legislation in March 2006, the Identity Cards Act, driven by the Tony Blair government.[467] It created national identity cards, a personal identification document, and a European Economic Area travel document, all linked to a database known as the National Identity Register.[468] However, there was opposition to the scheme.[469] The Identity Cards Act was repealed in December 2010, shortly after David Cameron's Conservative Party won the general election in the same year.[470]

In August 2017, the Indian Supreme Court delivered a major ruling on privacy rights in *Puttaswamy v. Union of India (Puttaswamy I)*.[471] In May 2007, India officially started its Multipurpose National Identity Card.[472] In August 2010, the national government in India launched the Aadhaar project, which created a national database of biometric (retina scans and fingerprints) and demographic information stored under a twelve-digit unique identification number for every resident in

[464] *See* THE DATA PROTECTION REGISTRAR, FIFTH REPORT OF THE DATA PROTECTION REGISTRAR, 1989, HC, at 5 (UK); *see also* Howe, *supra* note 457, at 353 (showing that the author served as Data Protection Registrar from 1984 to 1994).

[465] *See* THE DATA PROTECTION REGISTRAR, TENTH REPORT OF THE DATA PROTECTION REGISTRAR, 1994, HC (UK).

[466] *See* Philip A. Thomas, *Identity Cards*, 58 MOD. L. REV. 702, 702 (1995); Francis G.B. Aldhouse, *Electronic Government: A UK Perspective*, 10 INT'L REV. L. COMPUTS. & TECH. 157, 157–58 (1996).

[467] Identity Cards Act 2006, c. 15 (U.K.).

[468] *Id.* at 1.

[469] Clare Sullivan, *The United Kingdom Identity Cards Act 2006-Civil or Criminal*, 15 INT'L J.L. & INFO. TECH. 320 (2007); David Wills, *The United Kingdom Identity Card Scheme: Shifting Motivations, Static Technologies, in* PLAYING THE IDENTITY CARD: SURVEILLANCE, SECURITY AND IDENTIFICATION IN GLOBAL PERSPECTIVE 163, 164–65 (Colin J. Bennett & David Lyon eds., 2008) [hereinafter PLAYING THE IDENTITY CARD] (discussing opposition from some of the Labor Party members, Conservative Party members, civil rights groups, as well as the public campaigns from the NO2ID group).

[470] Identity Documents Act 2010, c. 40 (U.K.).

[471] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 [hereinafter *Puttaswamy I*]. For commentary, see Menaka Guruswamy, *Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors, Writ Petition (Civil) No. 494 of 2012*, 111 AM. J. INT'L L. 994 (2017).

[472] Taha Mehmood, *India's New ID Card: Fuzzy Logics, Double Meanings and Ethnic Ambiguities, in* PLAYING THE IDENTITY CARD, *supra* note 469, at 112–27.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

India.[473] The government mandated that Aadhaar data be linked to citizens' information from bank accounts, tax filings, medical records, and phone numbers.[474]

In a nine-judge panel, the Indian Supreme Court unanimously ruled in favor of privacy and held that Article 21 of the Indian Constitution protects privacy as a fundamental right in India.[475] The court specifically embraced the notion of informational self-determination when it declared that "[p]rivacy safeguards individual autonomy and recognizes the ability of the individual to control vital aspects of his or her life."[476] One year later, the case was brought to the Indian Supreme Court and again in *Puttaswamy II*, the constitutionality of the Aadhaar Act was challenged.[477] The Court upheld the statute.[478]

C. East Asian Democracies

The doctrine of informational self-determination has also spread to a number of East Asian democracies—Japan, South Korea, and Taiwan. What the three jurisdictions share is that privacy was not enumerated in the text of their constitutions. Therefore, it was the judiciary who recognized and created such a constitutional doctrine in their legal systems. All three jurisdictions are heavily

[473] *See generally* Amba Utara Kak & Swati Malik, *Privacy and the National Identification Authority of India Bill: Leaving Much to the Imagination*, 3 NUJS L. REV. 485 (2010) (discussing the National Identification Authority Bill of India, August 2010); Usha Ramanathan, *A Unique Identity Bill*, ECON. & POL. WKLY., July 24–30, 2010, at 10; Caroline E. McKenna, Note, *India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System*, 38 BROOK. J. INT'L L. 729, 731–32 (2013); Anvitha Sai Yalavarthy, Note, *Aadhaar: India's National Identification System and Consent-Based Privacy Rights*, 56 VAND. J. TRANSNAT'L L. 619 (2023).

[474] *See* ALAN GELB & ANNA DIOFASI METZ, IDENTIFICATION REVOLUTION: CAN DIGITAL ID BE HARNESSED FOR DEVELOPMENT? 171 (2018); N.S. RAMNATH & CHARLES ASSISI, THE AADHAAR EFFECT: WHY THE WORLD'S LARGEST IDENTITY PROJECT MATTERS (2018); Madison Julia Levine, Comment, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, 73 U. MIAMI L. REV. 618 (2019).

[475] *Puttaswamy I*, *supra* note 471, at 262 ("Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution.").

[476] *Id.* at 263.

[477] Unreported Judgments, Writ Petition (Civil) No. 494 of 2012, decided on Sept. 26, 2018 (SC), 1 [hereinafter *Puttaswamy II*]. The ruling of *Puttaswamy II* was further confirmed in *Mathew v. South Indian Bank Ltd.*, 2019 SCC Online SC 1456 (India).

[478] *Puttaswamy II*, *supra* note 477, at 394–411.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

influenced by the German right to personality theory (*jinkaku-ken*人格権) in interpreting privacy.

Japan was the first to introduce the notion into domestic constitutional discourse in East Asia. Professor Kōji Satō (佐藤幸治), studied in the United States in 1967 and thus was exposed to the country's privacy debates, particularly those of Alan F. Westin.[479] When he returned to Japan, Satō adopted Charles Fried's notion of privacy as the right to control one's own data (自己情報コントロール権) in an article published in 1970.[480] As an influential constitutional law professor at Kyoto University, Satō made the theory popular in Japan, including among privacy advocates and civil liberty groups.[481]

However, the Supreme Court of Japan has not yet recognized this theory. On two occasions, the Supreme Court turned down the invitation to incorporate such a theory.[482] The first occasion was in March 2008, in the *Juki Net Case*, where citizens, activists, and their support groups filed lawsuits, contending that the Juki Net Law—a centralized residence registration system—was in violation of Article 13 of the Japanese Constitution.[483] In the *Juki Net Case*, the Supreme Court confirmed that Article 13 of the Constitution does protect citizens' privacy; however, it also ruled that residents did not have a reasonable expectation of privacy.[484] The second occasion was in March 2023, in the *My Number Case*, where citizens challenged the

---

[479] *The Right of Self-Control and the Future of Protection of Personal Information*, HH NEWS & REPS., https://www.hummingheads.co.jp/reports/interview/s091007/interview43_01.html [https://perma.cc/5FP2-EL48] (last updated July 20, 2010).

[480] Kōji Satō,「プライヴァシーの権利（その公法的側面）の憲法論的考察（一）――比較法的検討――」 [*A Constitutional Examination of the Right to Privacy (Its Public Law Aspects) (Part 1)—A Comparative Legal Examination*], 86 KYOTO L. REV. 1, 12 (1970). I examined Professor Kōji Satō's contribution to the development of privacy as a constitutional right in Japan in a previous Article. *See* Dongsheng Zang, *Privacy and National Politics: Fingerprint and DNA Litigation in Japan and the United States Compared*, 43 PACE L. REV. 255, 273–77 (2023).

[481] *See id.*

[482] Saikō Saibansho [Sup. Ct.] Mar. 6, 2008, 62 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHŪ] 665 (Japan); Saikō Saibansho [Sup. Ct.] Mar. 9, 2023, Reiwa 4 (O) 39, 77 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHŪ] 627, https://www.courts.go.jp/app/hanrei_jp/detail2?id=91846 [https://perma.cc/SLR6-8LHR] (Japan).

[483] Saikō Saibansho [Sup. Ct.] Mar. 6, 2008, 62 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHŪ] 665 (Japan).

[484] *Id.* For commentary on the *Juki Net Case*, see Shigenori Matsui, *Is "My Number" Really My Number?: National Identification Numbers and the Right to Privacy in Japan*, 47 SYRACUSE J. INT'L L. & COM. 99 (2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

"My Number" national identification system introduced in 2015.[485] The Supreme Court, again, did not find violation of Article 13.[486] However, "My Number" remains a highly contested issue in Japanese society. In June 2023, the ruling party's approval rating reached a new low point, in part because of widespread privacy concerns of the "My Number" system.[487] The case is likely to come back to court in the future.

In South Korea, the idea of privacy rights was first introduced as a constitutional right in the 1970s, fighting the authoritarian regime of Park Chung Hee.[488] In 1987, South Korea ended its authoritarian era and transitioned to a democracy.[489] The doctrine of informational self-determination was recognized in 1998 by the Supreme Court case on the Resident Registration Network, where the South Korean Supreme Court held that "these constitutional provisions not only guarantee the right to be let alone, which protects personal activity from invasion by others and public exposure, but also an active right to self-control over his or her personal information in a highly informatized modern society."[490] In the 2005 *Fingerprint Case*,[491] the South Korea Constitutional Court ruled that self-determination regarding personal data is the right of the data subject "to determine to whom and in what scope her information is exposed and used" as a "basic right that is not enumerated in the Constitution."[492]

---

[485] Saikō Saibansho [Sup. Ct.] Mar. 9, 2023, Reiwa 4 (O) 39, 77 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHŪ] 627, https://www.courts.go.jp/app/hanrei_jp/detail2?id=91846 [https://perma.cc/SLR6-8LHR] (Japan).

[486] *Id.*

[487] *August Opinion Polls Find Low Popularity for Kishida as He Ends His Term*, NIPPON.COM (Aug. 30, 2024), https://www.nippon.com/en/japan-data/h30004/ [https://perma.cc/2JKN-CMTU].

[488] Woong Cheol Go, 人格権概念に関する一考察—日仏韓の比較法的研究から（東京大学博士学位論文） [An Examination of the Concept of Right to Personality—Comparing Japanese, French and Korean Law] (Sept. 30, 2014) (Ph.D. thesis, Tokyo University) (online).

[489] *See, e.g.*, Han Sung-Joo, *South Korea in 1987: The Politics of Democratization*, 28 ASIAN SURV. 52, 52 (1988).

[490] ACCESS CONTESTED, *supra* note 427, at 358 (quoting Daebeobwon [S. Ct.], July 24, 1998, 96Da42789 (S. Kor.)).

[491] Hunbeobjaepanso [Const. Ct.], May 26, 2005, 2004Hunma190 (S. Kor.).

[492] Il Hwan Kim, *Cooperation in the Field of Personal Data Protection: One World, One Standard?*, *in* THE EUROPEAN UNION AND SOUTH KOREA: THE LEGAL FRAMEWORK FOR STRENGTHENING TRADE, ECONOMIC AND POLITICAL RELATIONS 229, 238–39 (James Harrison ed., 2013).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

Like South Korea, Taiwan ended its authoritarian era in 1987 and has since transitioned to a democracy.[493] In December 2004, the Constitutional Court was presented a privacy case under Taiwan's Constitution.[494] It was on this occasion that the Taiwanese Constitutional Court embraced the doctrine of informational self-determination when it stated:

> The right of privacy, though not clearly enumerated under the Constitution, is an indispensable fundamental right protected under Article 22 of the Constitution because it is necessary to preserve human dignity, individuality, and the wholeness of the development of personality, as well as to safeguard the freedom of private living space from interference and the freedom of self-control of personal information . . . .[495]

In August 2022, the Constitutional Court again ruled in favor of privacy rights in the *Healthcare Database Case*, where citizens challenged laws in Taiwan that allowed government agencies to permit third-party researchers to have access to information in the national healthcare database without citizens' consent.[496] The Constitutional Court embraced the doctrine of informational self-determination and found the law in violation of the Constitution.[497]

In sum, the doctrine of informational self-determination has been officially adopted in both Taiwan and South Korea. In Japan, even though not officially adopted by the judiciary, it has gained widespread recognition in academic circles and popular support among citizens and privacy advocates.

CONCLUSION

It has been half a century since the United States Congress passed the Privacy Act of 1974 and led a revolution on the notion of privacy. The Act recognized that an individual should have the right to control the data about herself, a consensus formed around 1971 at the Senate hearings and passed into law in 1974. What was envisioned in the 1974 Act was essentially a bill of rights for the computer age. In

---

[493] *See, e.g.*, Jim W. Ko, *Cold War Triumph? Taiwan Democratized in Spite of U.S. Efforts*, 36 CASE W. RSRV. J. INT'L L. 137, 137 (2004).

[494] No. 585, Scope of Legislative Authority Case, 2004 LEADING CASES OF THE TAIWAN CONST. CT. 25 (Taiwan Const. Ct. Dec. 15, 2004), https://cons.judicial.gov.tw/en/docdata.aspx?fid=100&id=310766 [https://perma.cc/UH4J-QSXZ].

[495] *Id.* at para. 25.

[496] Jixun v. Ziyin, 2022 CONST. CT. INTERP. 111 (Const. Ct. Aug. 12, 2022) (Taiwan).

[497] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu

subsequent years, while the 1974 Act was substantially undercut in federal courts in the United States, the revolutionary notion of privacy became the foundation for data protection laws in continental Europe and commonwealth countries. It gained explicit constitutional status from judicial rulings in Germany, India, South Korea, and Taiwan, through the doctrine of informational self-determination. By contrast, today, an American bill of rights on data remains unfinished business at home.

This Article draws lessons from the recent past, especially in the context of AI regulation debates now. First, current controversies in the United States on whether to regulate AI are based on the premise that the tech companies are the main target of critiques. In July 2023, President Biden convened seven of the largest AI companies to the White House to secure voluntary commitments from them.[498] From the history and experience of the 1974 Act, however, it is obvious that the governmental agencies are by no means impartial regulators. They are an interested party in the debates, with their own incentives in the development and deployment of the AI technology. They are the "guardians" who must be guarded against. Second, the current controversies are exclusively focused on whether to lay down certain legal frameworks for regulating AI, while the function of the judiciary is very much out of the picture. From the history and experience of the 1974 Act, however, the federal courts played a critical role in fulfilling the promises in legislation passed by Congress. In passing the 1974 Act, Congress clearly regarded privacy rights as constitutionally protected legal rights of citizens. As has been shown, Senator Sam J. Ervin, Jr. chaired the Subcommittee on Constitutional Rights of the Senate Judiciary Committee. Under his leadership, the Subcommittee finished a report—*Federal Data Banks and Constitutional Rights*—shortly before the congressional vote on the 1974 Act.[499] However, the judiciary not only failed to give it any constitutional recognition, but also watered down the 1974 Act itself. As technology continues to evolve, privacy concerns are only becoming more dire. What is needed today is a genuine bill of rights for personal data—in the constitutional sense, a decisive shift from the past. That perhaps would require much more political mobilization. Before that constitutional commitment, the 1974 Act remains an unfinished business.

[498] Michael D. Shear, Cecilia Kang & David E. Sanger, *Pressed by Biden, Big Tech Agrees to A.I. Rules*, N.Y. TIMES (July 22, 2023), at A1.

[499] *Supra* note 250.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2024.1051
http://lawreview.law.pitt.edu