A MORE PERFECT PRIVACY

DANIELLE KEATS CITRON*

ABSTRACT

Fifty years ago, federal and state lawmakers called for the regulation of a criminal justice "databank" connecting federal, state, and local agencies. There was bipartisan concern that the system imperiled constitutional commitments and people's crucial life opportunities, including jobs, education, housing, and licenses. Bipartisan congressional concerns of the 1970s should be cause for reinvigoration, not resignation. Recounting the insights of members of the 93rd and 94th Congresses should embolden us. Their concerns clarify the headwinds that reformers face. Then, as now, powerful interests want us to think that privacy and public safety are incompatible. They want us to view diminished expectations of privacy as acceptable, even valuable. Revisiting this history should remind the public that totalizing surveillance is neither acceptable nor desirable. Privacy can and should be ours.

* Jefferson Scholars Foundation Schenck Distinguished Professor in Law, Caddell & Chapman Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; and 2019 MacArthur Fellow. Enormous thanks to Woodrow Hartzog and the Boston University Law Review for convening members of the privacy community to take stock of this current moment; to Minás Rasoulis for superb editing; to Barry Friedman, Ari Waldman, Ryan Calo, and Neil Richards for their insightful comments; and to Billi Jo Morningstar and Jeff Stautberg for superb editing and research.

CONTENTS

INTRODUCTION

Fifty years ago, federal and state lawmakers called for the regulation of a "databank" connecting federal, state, and local agencies. There was bipartisan concern that the system imperiled constitutional commitments and people's crucial life opportunities, including jobs, education, housing, and licenses. Congress held days (and days) of hearings over two years. Members warned of the threat of the "dossier dictatorship." Bipartisan bills proposed procedural and substantive restrictions. A resounding theme was that the computer system needed to be brought in line with American values.

What computer system sparked the legislative outrage and effort? The Federal Bureau of Investigation's ("FBI") National Crime Information Center's ("NCIC") computerized system enabling the sharing of personal data related to suspected criminal activity.[1] NCIC shared information about "wanted and missing persons" and "stolen property such as motor vehicles, boats, guns, securities, and license plates."[2] It distributed criminal history on offenders whose records were entered into the system by the state.[3]

Today, NCIC is relatively uncontroversial. Pursuant to federal regulation, personal data can be included in the system if reasonable suspicion exists that an individual is involved in criminal conduct.[4] The system is not totally free from concern: the FBI has been criticized for impermissibly including "civil

[1] LOUISE BECKER, CONG. RSCH. SERV., IB76004, CRIMINAL JUSTICE INFORMATION SYSTEMS 1 (1977).

[2] *Id.*

[3] DONALD A. MARCHAND, THE POLITICS OF PRIVACY, COMPUTERS, AND CRIMINAL JUSTICE RECORDS: CONTROLLING THE SOCIAL COSTS OF TECHNOLOGICAL CHANGE 134 (1980).

[4] Criminal Intelligence Systems Operating Policies, 45 Fed. Reg. 61612 (Sept. 17, 1980) (codified at 28 C.F.R. § 23) ("A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."); Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies, 58 Fed. Reg. 48448 (Sept. 16, 1993) (codified at 28 C.F.R. § 23) (updating funding guidelines, definitions, and Attorney General waiver provision); Criminal Intelligence Sharing Systems; Policy Clarification, 63 Fed. Reg. 71752 (Dec. 30, 1998) (codified at 28 C.F.R. § 23) (clarifying that information related to identification of criminal suspects may be included in NCIC but may not be used as independent basis for reasonable suspicion of involvement in criminal activity, and that nonintelligence information is not covered by regulation even if criminal-intelligence systems access such sources during searches on criminal suspects).

immigration information,"[5] and local police officers have been rebuked for using the system for personal reasons.[6] But the outrage has certainly dimmed.

In the United States, the quantity of personal data collected, used, shared, sold, and stored has grown to the point of international embarrassment.[7] NCIC is one node in the criminal justice and intelligence "information sharing environment."[8] Private- and public-sector databases reveal the most intimate details of people's lives, including their thoughts, searches, browsing habits, bodies, health, sexual orientation, gender, sexual activities, and close relationships.[9] The quantity and quality of personal data being amassed has exceeded all warning; the distinction between public and private collection efforts has vanished; the privacy that people want, expect, and deserve has been, and continues to be, under assault.[10]

Congressional debates of the past provide a lens into the present. Those debates remind us that the fight for privacy is just, righteous, and perilous. Powerful entities have influenced social attitudes, inducing the public into believing that indiscriminate surveillance is normal. People are told that data collection and sharing makes life better, safer, and more enjoyable.[11] Entities that accrue money and power from our personal data want us to think that nothing can be done, that privacy's time has passed, and that we should be satisfied with the status quo (or at least be mollified by thin procedural

[5] *Justice Department Is Misusing Criminal Database To Unlawfully Target Immigrants, Coalition Lawsuit Charges*, ACLU (Dec. 17, 2003, 12:00 AM), https://www.aclu.org/press-releases/justice-department-misusing-criminal-database-unlawfully-target-immigrants-coalition [https://perma.cc/5UWQ-LUSB] (describing federal lawsuit challenging state and local police use of NCIC to enforce federal immigration laws).

[6] *See, e.g.*, Timothy B. Lee, *Here's What Can Go Wrong When the Government Builds a Huge Database About Americans*, WASH. POST (July 8, 2013, 10:14 AM), https://www.washingtonpost.com/news/wonk/wp/2013/07/08/heres-what-can-go-wrong-when-the-government-builds-a-huge-database-about-americans/; Sadie Gurman & Eric Tucker, *Across US, Police Officers Abuse Confidential Databases*, ASSOCIATED PRESS (Sept. 28, 2016, 12:28 AM), https://apnews.com/general-news-699236946e3140659fff8a2362e16f43 [https://perma.cc/3DCV-YSZ2]. Under the Privacy Act of 1974, law enforcement can adopt rules that exempt databases from having to comply with the law. 5 U.S.C. § 552(b). In 2003, the FBI published a rule that exempted NCIC from the accuracy requirements of the Privacy Act. 28 C.F.R. § 16.96(g)(1) (2024).

[7] See DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 57 (2022).

[8] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011).

[9] *Id.* at 1451.

[10] *See id.* at 1451-52 (explaining how public and private entities collect and share data with each other).

[11] *See* NEIL RICHARDS, WHY PRIVACY MATTERS 207-08 (Oxford Press ed. 2022). Or, as Dave Eggers ominously wrote in *The Circle*, data sharing is caring. DAVE EGGERS, THE CIRCLE 305 (2013).

protections).[12] Congressional leaders of the past would have rejected this situation as unconstitutional and un-American. Revisiting this history does not mean that current practices should be sustained. Instead, it is to remind the public that totalizing surveillance is neither acceptable nor desirable. Privacy can and should be ours.

Part I revisits the congressional debates about NCIC from the 1970s. Part II highlights some lessons learned from those debates. Looking back to the debates of the 1970s helps chart a path forward. Legislative proposals from the 93rd and 94th Congress highlighted both procedural and substantive protections.[13] Procedural protections were not sufficient then, and they are not now.[14] In the past fifty years, the Information Privacy Law Project has reinforced why privacy matters and how the law can protect it.[15] Current federal efforts reflect this thinking, incorporating guardianship duties for public and private data handlers.[16] A reckoning with the Information Privacy Law Project's long-standing concerns is overdue, and it is in reach.

I. CONGRESSIONAL DEBATES OF THE 1970S

In the late 1960s and early 1970s, Congress devoted considerable attention to the "databank" problem.[17] On February 23, 1971, Senator Sam Ervin of North Carolina, chair of the Senate Judiciary Subcommittee on Civil and Constitutional Rights, called to order a hearing by explaining that "Americans

[12] *See* RICHARDS, *supra* note 11, at 1-2 (emphasizing public commentary that "privacy is dead").

[13] *See Dissemination of Criminal Justice Information: Hearings Before the Subcomm. on C.R. & Const. Rts. of the Comm. on the Judiciary*, 93d Cong. 2-17 (1973) (describing procedural safeguards of proposed bills for disseminating criminal justice information).

[14] As Woodrow Hartzog has wisely underscored! *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 56-57 (2018) (highlighting how Fair Information Practices are inadequate in addressing modern privacy problems); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 964-72 (2017) (same).

[15] Neil Richards coined the phrase "Information Privacy Law Project" to refer to the "collective effort by a group of scholars to identify a law of 'information privacy' and to establish information privacy law as a valid field of scholarly inquiry." Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006); *see also* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 197 (1995) (discussing information privacy law entrepreneurs). *See generally* COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008) (describing role and efforts of privacy advocates).

[16] *See generally* Julie M. Haney, Sandra Spickard Prettyman, Mary F. Theofanos & Susanne M. Furman, *Data Guardians' Behaviors and Challenges While Caring for Others' Personal Data*, *in* HCI FOR CYBERSECURITY, PRIVACY AND TRUST 163 (Abbas Moallem ed., 2023) (studying responsibilities of those handling personal data).

[17] *See* ARYEH NEIER, DOSSIER: THE SECRET FILES THEY KEEP ON YOU 99-100 (1975) (recounting speech in which President Nixon spoke about proposed legislation that would govern collection of criminal justice information).

in every walk of life are concerned about the growth of government and private records on individuals."[18] Senator Barry Goldwater of Arizona asked: "Where will it end? . . . Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?"[19] Senator Charles H. Percy of Illinois noted:

> I hope that we never see the day when a bureaucrat in Washington or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear that is the trend. . . . Federal agencies have become omnivorous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files . . . of unprotected information on millions of Americans.[20]

Of particular concern were databases of criminal justice information, notably NCIC, a "law enforcement information network" for local, state, and federal agencies.[21] Established by Attorney General Ramsey Clark in 1967, NCIC was taken over by the FBI in 1970.[22] By 1972, forty state and metropolitan agencies joined NCIC,[23] which enabled agencies to share and access information about "wanted and missing persons" and stolen property, such as cars, boats, and guns.[24] NCIC linked to the "criminal history on each offender whose record was entered into the system by the states."[25]

Beyond tracking agency uses of the system, NCIC had few restrictions.[26] This was unsurprising given that law enforcement officials dominated the NCIC

---

[18] FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 179-80 (2009).

[19] 120 CONG. REC. 36,917 (1974) (statement of Sen. Goldwater), *reprinted in* JOINT COMM. ON GOV'T OPERATIONS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 805 (1976) [hereinafter SOURCE BOOK ON PRIVACY].

[20] 120 CONG. REC. 36,917 (1974) (statement of Sen. Percy), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 19, at 776.

[21] BECKER, *supra* note 1, at 1 ("The development and automation of criminal justice information systems . . . have cause considerable concern.").

[22] Congress did not need to authorize the NCIC because the Attorney General took the position that the 1930 federal statute authorizing the FBI to collect and share "identification and other records" related to crime to federal, state, and local agencies provided the legal foundation for the system. ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY 52-53 (1972).

[23] *Id.* at 54 (describing operations of NCIC, where system "was running 24 hours a day, seven days a week, with about 76,000 'network transactions' handled daily").

[24] BECKER, *supra* note 1, at 1.

[25] MARCHAND, *supra* note 3, at 137. Records included personal identification information, arrest charges, disposition of cases, custody history, and supervision status. *Id.*

[26] *See* WESTIN & BAKER, *supra* note 22, at 56.

advisory board.[27] FBI Director J. Edgar Hoover told the public that NCIC "meant only 'good things' . . . for 'the average, law-abiding citizen'" because it only included information about serious crimes.[28] "[N]obody can misuse the NCIC data banks to embarrass you with some ancient traffic violation or tidbit of personal [gossip] . . . . No such information will be stored there," Hoover maintained.[29]

Congress was not mollified by Hoover's assurances.[30] In the 93rd Congress, Senate and House judiciary subcommittees held hearings devoted to criminal justice information amassed in computerized systems and shared with public and private entities.[31] Policymakers expressed grave concerns, sounding themes that would recur in the information privacy law community for fifty years.[32]

An initial objection was that the FBI had rushed to computerize criminal justice information without proof of concept or an explanation of how "traditional values" would be safeguarded.[33] Senator Charles Mathias of Maryland, for instance, expressed frustration that the FBI received funding for NCIC before a "philosophy for its use was formulated."[34]

---

[27] *Dissemination of Criminal Justice Information*, *supra* note 13, at 213 (noting "inherent conflict of interest in allowing this massive system, that affects the lives of every citizen, to regulate itself").

[28] WESTIN & BAKER, *supra* note 22, at 52 (describing Hoover's 1966 articles guaranteeing "no intrusion whatsoever" on privacy).

[29] *Id.* at 53 (alterations in original).

[30] Courts also were not satisfied with Hoover's assurances. *See* Menard v. Mitchell, 328 F. Supp. 718, 727 (D.D.C. 1971). Individuals sued the FBI to prevent them from sharing their arrest records with employers. *Id.* Federal district court Judge Gerhard Gesell ruled that the FBI could not release a plaintiff's arrest record to private employers. *Id.* Judge Gesell declared: "[W]ith the increasing availability of fingerprints, technological developments, and the enormous increase in population, the system is *out of effective control*. The Bureau needs legislative guidance and there must be a national policy developed in this area which will have built into it adequate sanctions and administrative safeguards." *Id.* (emphasis added). The court maintained that the FBI was "without authority to disseminate arrest records outside the Federal Government for employment, licensing or related purposes whether or not the record reflects a later conviction." *Id.* The FBI complied with the ruling by suspending sharing of criminal records for employment and licensing checks. WESTIN & BAKER, *supra* note 22, at 61. However, in September 1971, Senator Alan Bible of Nevada introduced a provision in an appropriation bill to authorize the FBI to continue circulating FBI records as they had before the *Menard* case; the rider was passed and signed by President Nixon. *Id.*

[31] MARCHAND, *supra* note 3, at 178 (noting Senator Ervin commenced six days of hearings on proposed bills in March 1974).

[32] *See* David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 69 (2013) (arguing concerns articulated by Information Privacy Law Project should inform how courts and lawmakers view Fourth Amendment commitments).

[33] *Id.*

[34] *Privacy: The Collection, Use, and Computerization of Personal Data: Joint Hearings Before Ad Hoc Subcomm. on Priv. and Info. Sys. of the Comm. on Gov't Operations and the Subcomm. on Const. Rts. of the Comm. on the Judiciary*, 93d Cong., 2d Sess. 11 (1974) (statement of Sen. Charles Mathias) (warning of new surveillance technology's threat to individual privacy).

Bipartisan concern emerged that NCIC undermined constitutional commitments. Restraining criminal justice databases was necessary "to secure the constitutional rights guaranteed by the first amendment, fourth amendment, fifth amendment, sixth amendment, ninth amendment, and fourteenth amendment."[35] Representative William Alexander, Jr. of Arkansas warned of the "chilling effect on the exercise of First Amendment rights."[36] Senator Sam Ervin warned that the power given to the government made a mockery of the Bill of Rights, turning them into "just . . . words:"[37]

> Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. . . . We should not have to conjure up 1984 or a Russian-style totalitarianism to justify protecting our liberties against Government encroachment. . . . Congress must act before those new systems are developed . . . . The peculiarity of those new complex technologies is that once they go into operation, it is too late to correct our mistakes or supply our oversight.[38]

Senator Barry Goldwater of Arizona warned: "Total control requires total information."[39] Furthermore, Senator Goldwater argued that information in government databases could be used to "manipulate . . . social conduct."[40] Professor Arthur Miller, a recurring witness, testified that: "Nineteen eighty-four is not a year, but a state of mind." He argued that federal law needed to strictly regulate government databases of personal information to avoid fulfilling Orwell's vision.[41]

Another shared concern was that inaccurate or incomplete criminal history information would damage people's reputations and livelihoods.[42] Representative Don Edwards of California, a former FBI special agent, underscored that arrest records are shared and used to suggest someone is "a job risk, credit risk, tenant risk or student risk. . . . These . . . records . . . injure people who have never been involved in any illegal or criminal act."[43] Echoing the testimony of Professor Miller, Representative Edwards warned that the "insatiable appetite . . . to collect every possible piece of information on every

---

[35] S. 2963, 93d Cong., § 101 (1974) (warning of potential dangers criminal justice information systems pose to American citizens).

[36] 93 Cong. Rec. 16373 (1970).

[37] *Criminal Justice Data Banks—1974: Hearings Before the Subcomm. on Const. Rts. of the Comm. on the Judiciary*, 93d Cong., 2d Sess. 16 (1974) (statement of Sen. Sam Ervin) (arguing that stripping privacy from citizens would also strip away their rights and privileges).

[38] *Id.* at 16-17 (statement of Sen. Sam Ervin).

[39] *Id.* at 141 (statement of Sen. Barry Goldwater).

[40] *Id.* (statement of Sen. Barry Goldwater) (demonstrating both importance and danger that total access to information poses).

[41] LANE, *supra* note 18, at 180 ("[Miller] urged the committee to propose strict regulations on the sharing of data by federal agencies and to advocate for an enforcement agency to monitor federal privacy practices.").

[42] *Dissemination of Criminal Justice Information*, *supra* note 13, at 78.

[43] 120 CONG. REC. 9352 (1974) (statement of Rep. Don Edwards).

possible citizen" would lock citizens into "record prisons."[44] This was especially true for Black individuals who were disproportionately arrested without reasonable suspicion or probable cause.[45]

State policymakers sounded similar alarms in congressional testimony. Massachusetts Governor Francis Sargent refused to connect his state's criminal justice databases to NCIC because it lacked privacy protections.[46] Under Massachusetts law, criminal justice databases could only store information related to criminal convictions and could only be shared with law enforcement agencies.[47] Governor Sargent explained that NCIC lacked those protections, fulfilling what he saw as "the technological nightmare of 1984."[48] He underscored the costs of an unregulated criminal justice records system. Governor Sargent talked about a man who received a pardon after serving his sentence. The man then moved to another state and enrolled in college. He was expelled after the college received a record of the man's felony conviction.[49] Although the Governor's office explained that the man had been pardoned, the college refused to readmit him. Governor Sargent criticized how NCIC records were used to deny people "a second chance."[50] This "is what happens when we elevate a system over the individual, a machine over man. This is the pain we cause when we allow our technology to run ahead of us, uncontrolled," Governor Sargent explained.[51]

Perhaps to deflect from the growing Watergate scandal, on February 23, 1974, President Richard Nixon gave a national radio address on "The American Right of Privacy."[52] He conveyed his concern that criminal justice databases embroiled citizens in a Kafka-esque nightmare: "In many cases, the citizen is not even aware of what information is held on record, and if he wants to find out, he either

[44] *Id.*

[45] *Dissemination of Criminal Justice Information*, *supra* note 13, at 107 ("The fact of an arrest, of course, establishes nothing about the person arrested except that some other person has accused him of criminal misconduct–a risk to which all persons are subject but to which members of several minority groups are disproportionately exposed.").

[46] The Nixon Administration tried to force Governor Sargent's hand by suing the state for refusing to join NCIC. *Criminal Justice Data Banks—1974*, *supra* note 37, at 51-54 (testimony of Governor Francis W. Sargent). The Defense Department froze 2,400 jobs in Massachusetts; the Small Business Administration threatened to withhold $30 million in disaster aid and loans to the state. *Id.* Attorney General Elliot Richardson dropped the federal suit against Massachusetts in September 1973, which was shortly before President Nixon fired him during the Midnight Massacre. *Id.* at 52.

[47] MARCHAND, *supra* note 3, at 146.

[48] *Criminal Justice Databanks—1974*, *supra* note 37, at 51.

[49] *Id.* at 53.

[50] *Id.*

[51] *Id.*

[52] NEIER, *supra* note 17, at 99; LANE, *supra* note 18, at 190 (outlining steps executive branch would take to address such topic). Irony, hypocrisy, and gaslighting were in abundance in that speech.

has nowhere to turn or else he does not know where to turn."[53] President Nixon told the nation that his newly created Domestic Council Committee on the Right of Privacy, a cabinet-level group, would suggest reforms to combat misuses of criminal history information.[54]

Members of Congress proposed criminal justice reform bills that included fair information practice principles ("FIPs") like securing a person's right to access and correct information.[55] Proposed legislation also included duties of confidentiality, limits on collection, and mandatory deletion of stale data. A bill sponsored by Representative Edwards provided that "no criminal data bank shall collect" personal data unless it concerned a person's "apprehension, adjudication, confinement, or rehabilitation" and had been "recorded" by an official agency.[56] Edwards' bill mandated the destruction of arrest records after two years and convictions after ten years. Civil penalties included equitable relief like putting agencies in a two-year time-out from collecting criminal justice data if they failed to comport with federal law.[57] Senator Barry Goldwater of Arizona argued that to secure individual "liberty," computers should be "programmed to erase unwanted . . . details" of individuals' pasts.[58]

Congress made progress on the broader question of government databases of personal information. On December 31, 1974, Congress passed the Privacy Act of 1974 ("Privacy Act"), which established FIPs for federal agencies.[59] Crucially, though, the law enabled law enforcement agencies to exempt themselves from the Privacy Act because separate legislation addressing criminal justice databases was in the pipeline.[60] Although Representative Goldwater boasted that the 93rd Congress would "earn the title of the 'Privacy Congress,'"[61] no criminal justice bill was passed in that session or successive sessions. Why not?

---

[53] NEIER, *supra* note 17, at 100.

[54] LANE, *supra* note 18, at 190.

[55] Although federal bills differed on the issue of which agency—federal, state, local, or independent board—would control and operate NCIC, they enjoyed bipartisan support. NEIER, *supra* note 17, at 100. Several bills would have permitted states to enact stricter protections. *Criminal Justice Information and Protection of Privacy Act of 1975: Hearings on S. 2008, S. 1427, and S. 1429 Before the Subcomm. on Const. Rts. of the S. Comm. on the Judiciary*, 94th Cong., 1st Sess. 1-2 (July 15, 1975).

[56] *Dissemination of Criminal Justice Information*, *supra* note 13, at 12-13 (discussing HR 9783).

[57] *Id.* at 17.

[58] *Criminal Justice Databanks—1974*, *supra* note 37, at 140-41 (statement of Sen. Goldwater).

[59] 5 U.S.C. § 552.

[60] *See* 5 U.S.C. § 552(b) (outlining exemptions).

[61] LANE, *supra* note 18, at 190.

Those bills failed due to the strong opposition of law enforcement agencies.[62] The Treasury Department, the Securities and Exchange Commission, the Federal Trade Commission, and the Department of Justice insisted that the proposed restrictions would make fighting crime impossible.[63] Deputy Attorney General Harold R. Tyler, Jr. argued that "intelligence really is gathered by little bits and pieces of information which flow from various people, various sources, both official and public, and sometimes an informer. Sometimes a scrap of information, as innocent as the report that somebody has entered a telephone booth, proves to be the most important."[64] The press also lined up against various bills on the grounds that restrictions undermined the public's right to know.[65]

The absence of criminal justice information reform was a sticking point for the Privacy Protection Commission ("Commission"), which was created by the Privacy Act to report on remaining concerns.[66] In 1977, the Commission issued its findings, criticizing the lack of any mechanism to ask whether a record-keeping system "should exist at all" and the "gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent."[67] The Commission underscored that law enforcement should only collect personal data if it is "authorized by a statute that details the purpose for the reporting and the standards of relevance for any information collected."[68] In its view, "voluntary disclosure by third party record keepers must be limited and (recommended) that the government use recognized by legal process to gain access to records."[69]

II. LESSONS FOR THE PRESENT

NCIC is one input of countless inputs into the federal government's "information sharing environment." Law enforcers, intelligence agencies, and state-local-federal fusion centers have been purchasing access to *everyone's*

[62] *Criminal Justice Information and Protection of Privacy Act of 1975*, *supra* note 55, at 1-2 (statement of Sen. Tunney).

[63] *Privacy: The Collection, Use, and Computerization of Personal Data*, *supra* note 34, at 193, 458, 463, 476, 480-84.

[64] *Criminal Justice Information and Protection of Privacy Act of 1975*, *supra* note 55, at 213 (testimony of Harold Tyler, Jr.).

[65] *Id.* at 284 (letter from the Am. Newspaper Publishers Ass'n) ("The intention of this bill is laudable: to further the protection of individual privacy. The result is lamentable: the placement of the public's business behind locked doors.").

[66] LANE, *supra* note 18, at 194 (noting Commission was a "paper tiger, since the legislation did not provide for any enforcement mechanisms").

[67] REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, THE PRIVACY ACT OF 1974: AN ASSESSMENT., app. 4, at 108, 114.

[68] SARAH P. COLLINS, CONG. RSCH. SERV., REP. NO. 79-236, THE PRIVACY PROTECTION STUDY COMMISSION: BACKGROUND AND RECOMMENDATIONS 52 (1979).

[69] *Id.* at 53.

personal data from private entities.[70] That includes cellphone app users' geolocations and thousands of other data points in data-broker dossiers.[71] If law enforcers access private systems without integrating personal data into their systems, then those actions may not be covered by federal regulation or law—leaving hardly any protection at all.[72]

One could view the public-private data grab with resignation. One could accept the argument that privacy reform is incompatible with efforts to protect national security and public safety. But that argument is neither descriptively accurate nor normatively desirable. Yes, we have normalized the idea that digital reservoirs of intimate data are inevitable *and* necessary.[73] Twenty-five years ago, Frederick Schauer warned that private-public surveillance practices could diminish our expectation of privacy.[74] Regrettably, Schauer was prescient. As Woodrow Hartzog, Evan Selinger, and Johanna Gunawan explain: "The more we are exposed, the less capacity we have for democratic resistance."[75] To riff on their point, the more that personal data is collected, used, and shared, the less capacity for resistance we *see in ourselves*.

Bipartisan congressional concerns of the 1970s should be cause for reinvigoration, not resignation.[76] Recounting the insights of members of the 93rd and 94th Congresses should embolden us. Their concerns clarify the headwinds that reformers face. Then and now, powerful interests want us to think that privacy and public safety are incompatible. They want us to view diminished expectations of privacy as acceptable, even valuable. Data brokers, online advertisers, and law enforcers have inculcated the view that our personal data

[70] Garance Burke & Jason Dearen, *How an Obscure Cellphone Tracking Tool Provides Police 'Mass Surveillance on a Budget'*, PBS NEWS HOUR (Sept. 1, 2022, 4:38 PM), https://www.pbs.org/newshour/politics/how-an-obscure-cellphone-tracking-tool-provides-police-mass-surveillance-on-a-budget [https://perma.cc/H7F6-YPL2] (noting federal oversight company's sale of cell phone tracking tool to law enforcement); Jessica Lyons Hardcastle, *Why Bother with Warrants When Cops Can Buy Location Data for Under $10k?*, REGISTER (Sept. 1, 2022, 8:28 PM), https://www.theregister.com/2022/09/01/eff_fog_data_broker/ [https://perma.cc/3HK9-JFPE] (highlighting law enforcement's ability to purchase private citizens' location data without warrant).

[71] CITRON, *supra* note 7, at 58-60.

[72] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE (2013); *see also* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1799 (2022).

[73] *See generally* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021) (detailing how the tech industry undermines privacy by manipulating how the public thinks about privacy); Evan Selinger & Judy Rhee, *Normalizing Surveillance*, 22 N. EUR. J. PHIL. 49 (2021) (explaining "normalization" of surveillance and its consequences in context of privacy rights).

[74] *See* Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS 555, 562 (1998).

[75] Woodrow Hartzog, Evan Selinger & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 WASH. U. L. REV. 717, 770 (2024).

[76] *See supra* Part I.

must be collected, used, and shared because it serves *them*.[77] As President Gerald Ford admitted to law students in 1975, privacy is under assault, and "'one of the worst offenders is the federal government itself.'"[78]

The Information Privacy Law Project has been building a case for meaningful reform.[79] Scholars and advocates have shown why privacy matters and how it should be protected.[80] They have explored the "damaging effects of surveillance on life projects central to personal liberty" and human dignity, including the chilling of self-development, self-expression, and relationships.[81] They have "warned about the stakes of broad and indiscriminate surveillance for a healthy democracy."[82] They have underscored the perils of governmental power gained through personal information—blackmail, discrimination, and persuasion.[83]

[77] *See* CITRON, *supra* note 7, at 8-11.

[78] LANE, *supra* note 18, at 195.

[79] *See* Richards, *supra* note 15, at 1089 (describing aims of the Information Privacy Law Project).

[80] *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1927-32 (2013).

[81] Gray & Citron, *supra* note 32, at 76. *See generally* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); RICHARDS, *supra* note 11; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION (2017); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE (2012); NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011); THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (SAUL LEVMORE & MARTHA C. NUSSBAUM EDS., 2010); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); PRIVACY: NOMOS XIII (J. ROLAND PENNOCK & JOHN W. CHAPMAN EDS., 1971); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1998); JULIE INNES, PRIVACY, INTIMACY, AND ISOLATION (1992); CHARLES FRIED, AN ANATOMY OF VALUES (1971); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); ALAN WESTIN, PRIVACY AND FREEDOM (1967). We owe a debt of gratitude to the scholars developing these themes, including the participants in the *Boston University Law Review* symposium. Capturing that literature in these footnotes would take me far over my word limit, so I shall just provide a taste. My gratitude to these scholars is deep and abiding.

[82] Gray & Citron, *supra* note 32, at 77; *see, e.g.*, Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 565-74 (1995).

[83] *See, e.g.*, RICHARDS, *supra* note 11, at 146-63; DAVID LYON, THE ELECTRONIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 83-101 (1994); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131, 134 (Austin Sarat ed., 2014).

They have developed our understanding of the broad array of privacy harms,[84] including the inextricable relationship between privacy and equality.[85]

Proposals from the past resonate with proposals of the present. Recall that in the 1970s, substantive restrictions on databases of personal data were on the table. Lawmakers have been listening to Information Privacy Law Project's arguments that entities handling personal data should act as the guardians of that data. For instance, the American Data Privacy and Protection Act of 2022 would have imposed a baseline duty to refrain from collecting personal data unless companies reasonably needed it to provide products or services to existing customers.[86] The Act would have made it much harder to collect and exploit intimate data—including health, genetics, biometrics, geolocation, sexual behavior, intimate images, online activities over time, private communications, and minors' data.[87] It would have held data collectors accountable for discrimination without proof of invidious intent.[88] We have serious bipartisan bona fides in steeling ourselves and demanding meaningful reform along these lines.

[84] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1144-52 (2011); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 794 (2022); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 3 (2014); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 2-13 (2011).

[85] *See, e.g.*, ALLEN, *supra* note 81, at 153-69 ; KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 32 (2017) (positing "disturbing equality problem" when those of low socioeconomic status are denied privacy rights); SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 17 (2015) (defining "digital discrimination" as differential application of surveillance technologies); SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 180-214 (2021) (suggesting doctrinal reforms to apply equal protection concepts to privacy tort of public disclosure of private facts); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L.J.F. 907, 911 (2022) (noting "pervasive calls for improved data-privacy governance, using the lens of race to magnify the consequences for African Americans" of surveillance capitalism); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 64 (2009) (arguing online publication of sensitive information "impair[s] victims' ability to participate in online and offline society as equals").

[86] Danielle Keats Citron & Alison Gocke, *Nancy Pelosi Is Blocking Landmark Data Privacy Legislation—For a Good Reason*, SLATE (Sept. 9, 2022, 5:50 AM), https://slate.com/technology/2022/09/nancy-pelosi-data-priavcy-law-adppa.html [https://perma.cc/YTD9-VXKW].

[87] *Id.*

[88] *Id.*