REVISITING THE PRIVACY ACT OF 1974 FOR BIG DATA POLICING

Sarah Lamdan*

CITE AS: 6 GEO. L. TECH. REV. 386 (2022)

TABLE OF CONTENTS

I. INTRODUCTION

What would you think if you were pursuing the news and you read the headline *New Privacy Law to Have Major Impact on Government Data*? A new privacy law may strike you as a much-needed response to the ways government entities are using personal data to track us and make data analytics-based decisions about our lives. Perhaps you would assume that the headline refers to a U.S. iteration of the European Union's General Data Protection Regulation (GDPR) or one of the many federal data privacy laws

* Sarah Lamdan is a Professor of Law at CUNY School of Law and author of the book "Data Cartels: The Companies that Control and Monopolize Our Information" (Stanford University Press, 2022). She has an information science degree focused on legal information management and is a senior fellow at SPARC (the Scholarly Publishing and Academic Resources Coalition), as well as a fellow at the Engelberg Center on Innovation Law and Policy at NYU School of Law.

proposed in Congress this session.[1] But this headline is not from today; it is from 1974 when Congress passed the Privacy Act.[2]

The 1970s-era law was meant to protect people's privacy in response to the rise of data collection and computer technologies. Fifty years ago, the public was already worried that the government would use personal data in ways that violate individuals' rights and liberties.[3] Data technologies were rapidly evolving, giving the government new tools for collecting, storing, and sorting people's data. At the same time, the Watergate scandal and Counterintelligence Program (COINTELPRO) revelations reminded people that the government could use personal data and technology to surveil them. In the midst of mass-datafication and government distrust, the Privacy Act was supposed to explicitly incorporate the penumbral privacy rights emanating from the Bill of Rights into our laws. Congress also intended to establish due process rules for the Government's use of computer technology for personal data systems.[4]

The Privacy Act was passed in response to civil rights concerns raised by surveillance and data analytics, but the law, which limits how the government can acquire and use our data,[5] is rarely, if ever, mentioned when people raise concerns about data-driven government surveillance today.[6] Even

---

[1] Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, International Association of Privacy Professionals (IAPP), https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ (last visited Aug. 2, 2021) [https://perma.cc/2GSR-AUR3].

[2] JOINT COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 1208 (Comm. Print 1976), https://www.justice.gov/opcl/paoverview_sourcebook/download [https://perma.cc/5KCF-WYQ9] [hereinafter *Source Book*].

[3] RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) [hereinafter *HEW Report*].

[4] *Source Book*, *supra* note 2, at 858-74 (referring to the penumbra of rights described in *Griswold v. Connecticut*, 381 U.S. 479 (1965)).

[5] *See, e.g., How Data-Driven Policing Threatens Human Freedom*, THE ECONOMIST (Jun. 4, 2018), https://www.economist.com/open-future/2018/06/04/how-data-driven-policing-threatens-human-freedom [https://perma.cc/9RBJ-U47W].

[6] The Privacy Act is not mentioned in the context of the NSA's data surveillance program, ICE's data-driven immigrant tracking schemes, or the Postal Services' social media data monitoring. *See*, *e.g.*, Ellen Nakashima, *NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says*, WASH. POST (June 29, 2021), https://www.washingtonpost.com/national-security/nsa-surveillance-xkeyscore-privacy/2021/06/29/b2134e7a-d685-11eb-a53a-3b5450fdca7a_story.html [https://perma.cc/KFP7-PWGC]; Johana Bhuiyan, *A US surveillance program tracks nearly 200,000 immigrants. What happens to their data?*, GUARDIAN (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap [https://perma.cc/YU29-KUHB]; Jana Winter, *The Postal Service is running a 'covert*

though the Act is left out of our current data surveillance policy discussions, its provisions were created to deal with the types of government surveillance fears people are talking about in our current digital era. The legislators who passed the Privacy Act hoped to prevent the government from using personal data to track people en masse and make decisions about their rights and privileges based on government data troves.

The Privacy Act was a reaction to predictions that have proven accurate. The law was based on research by experts like James B. Rule, a sociologist specializing in privacy and information, who correctly imagined how our data would be used in decision-making analytics and as a tool for exerting social control.[7] Rule knew that, with data technologies, the government would be able to quickly single out a minority of people who pose some sort of social "risk." Rule foresaw how data would be used to justify action against those people.[8] He also predicted that quick and cheap access to automated data files would lead organizations to indulge in "dragnet behavior," using data systems to screen the entire population's data in order to discover a few members with specified characteristics.[9] The law is also based on data conventions—like the Fair Information Practice Principles—that have persevered as best practices in the modern era.[10]

---

operations program' that monitors Americans' social media posts, YAHOO! NEWS (Apr. 21, 2021), https://news.yahoo.com/the-postal-service-is-running-a-running-a-covert-operations-program-that-monitors-americans-social-media-posts-160022919.html.News [https://perma.cc/SAJ6-DN96].

[7] *See generally*, JAMES B. RULE, https://www.jamesbrule.net/ [https://perma.cc/6W4J-793J] (last visited Apr. 25, 2022).

[8] JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE, 1973. "Risk" is the common term used by analytics companies to describe what their data systems identify and cull out from people's personal data dossiers. *See, e.g.*, LexisNexis, *About LexisNexis*, https://www.lexisnexis.com.hk/about-us/overview [https://perma.cc/46F5-JSHB]; Thomson Reuters, *Who We Serve*, https://www.trssllc.com/government-2/ [https://perma.cc/9LHW-J7RJ] (last visited November 14, 2021); LexisNexis*, Industries We Serve*, https://www.lexisnexisspecialservices.com/who-we-are/industries/ [https://perma.cc/LT87-PZCT].

[9] *HEW Report*, *supra* note 3, at 15.

[10] The Fair Information Practice Principles have even been enshrined in U.S. law and policy. The Federal Trade Commission applies them to address online data privacy issues, and they are at the foundations of California's Consumer Privacy Act. *See* Federal Trade Commission, Self-Regulation and Privacy Online: A Report to Congress, Jul. 1, 1999, https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf. [https://perma.cc/E2GQ-FAKC]; Ronald R. Raether, Jr. et al., *Data Processing Obligations: Virginia Consumer Data Protection Act Series*, TROUTMAN PEPPER (Mar. 25, 2021), https://www.troutman.com/insights/virginia-consumer-data-protection-act-series-data-processing-obligations.html [https://perma.cc/3BZM-92K2].

Although Rule's assumptions have proven true, the law meant to deal with Rule's predictions has been largely forgotten. Instead of focusing on the Privacy Act, Congress is inventing entirely new laws to deal with the same personal data problems that it already dealt with in 1974. As we consider new laws that address data surveillance and predictive software-based law enforcement problems, we don't have to leave the original Privacy Act behind. Many of its provisions could be given new life to meet the challenges of today's data problems. This essay will look at how the Privacy Act was intended to work and suggest that instead of making an entirely new legal regime to deal with government data brokering, we revisit this well-researched and carefully-conceived information law.[11]

II. THE HISTORY OF THE PRIVACY ACT OF 1974

The Privacy Act was enacted to prevent the government from secretly stockpiling our data and using it as a tool to spy on us and otherwise infringe on our civil liberties.[12] It was passed on the heels of two scandals—Watergate and COINTELPRO—where people deemed "subversive" were surveilled and targeted by political operatives and police.[13] In the 1970s, people were rightfully suspicious of the government using communication technologies like tape recordings, phone wiretapping, and other surveillance devices to spy on and track private citizens.

At the same time that people were increasingly distrustful of government, data technologies were rapidly evolving. In 1970, Edgar Codd wrote a paper describing relational, shared data banks that spurred the database systems that we are familiar with today.[14] Dialog, the first database search system, allowed people to search digitized material with command language

---

[11] This Privacy Act essay is the prequel to a more in-depth article that will be co-written with Daniel Amar Peña, Staff Attorney at Bronx Defenders.

[12] THE PRIVACY ACT OF 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974), is part of a constellation of information laws that were passed or amended in the early 1970's during an era when technological change and political strife made people desire more government transparency, more protection from government surveillance, and more rules around how the government uses computer technologies. The other information laws include Freedom of Information Act, 5 U.S.C. §552 (1974); Presidential Records Act, 44 U.S.C. §§ 2201-07 (1978), and the first federal records law, Federal Records Act, 44 U.S.C. §3101 (1950).

[13] The Privacy Act's principal sponsor, Senator Sam Ervin, summarized the need for the law by saying that "[i]f we have learned anything in this last year […], it is that there must be limits upon what the Government can know about each of its citizens." *Source Book*, *supra* note 2, at 4. *See also* U.S. DEP'T OF JUSTICE, Overview of the Privacy Act of 1974 (2020), https://www.justice.gov/Overview_2020/download [https://perma.cc/J5ZX-MV9K].

[14] Edgar Codd, *A Relational Model of Data for Large Shared Data Banks*, 13 COMMC'NS OF THE ACM, 377 (1970).

for the first time.[15] In short, the 1970s were when data started being not just something to collect, but something malleable and searchable. Data was no longer static information—it was a dynamic material that could be sorted and structured with more nuance. New data inventions spurred our modern, fast-expanding tech industry. In 1975, Gordon Moore predicted that technological innovation would continue to evolve exponentially, with computing power doubling every few years.[16]

With the knowledge that the use of data and computer systems would only increase, Congress relied on the expertise of information science scholars and researchers, as well as data system operators, users, and subjects who served on the Department of Health, Education, and Welfare (HEW) advisory committee that drafted the Fair Information Practice Principles.[17] The Fair Information Practice Principles distilled years of extensive information science and policy research into recommendations on how best to protect people's privacy in a world where paper-based systems of information creation, storage, and retrieval were being replaced with electronic informational technologies.[18] The Privacy Act was supposed to provide data due process by:

- guaranteeing that the government would not keep systems of personal data records whose very existence is secret;
- ensuring that people can determine what records pertaining to them are collected, maintained, used, or disseminated by an agency;
- requiring agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes;
- affording individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and
- instructing agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately.[19]

III. THE PRIVACY ACT FIFTY YEARS LATER

Even though the Privacy Act became law, we are still struggling to regulate the government's use of personal data. Instead of becoming more

---

[15] *Dialog Online Search System, 1966*, ENGINEERING AND TECHNOLOGY HISTORY WIKI (2019), https://ethw.org/Milestones:DIALOG_Online_Search_System,_1966 [https://perma.cc/DNE7-FY8Z].

[16] Gordon E. Moore, Co-founder, Intel Corporation, IEEE Text Speech: Process In Digital Integrated Electronics (1975), https://www.eng.auburn.edu/~agrawvd/COURSE/E7770_Spr07/READ/Gordon_Moore_1975_Speech.pdf [https://perma.cc/4EWW-6Z3T].

[17] *HEW Report*, *supra* note 3, at ix.

[18] U.S. DEP'T OF JUSTICE, *supra* note 13, at 1.

[19] *HEW Report*, *supra* note 3, at xx–xxi.

transparent and interactive, the government's use of data-based decision making and surveillance has become more opaque and secretive, especially in law enforcement agencies. Entire books have been written about the constitutionally-fraught dangers of big data policing, the injustices it causes, and the constitutional concerns it raises.[20]

The data privacy concerns haven't changed since the 1970s, but data technologies have changed dramatically. Human intelligence-based policing used to be the primary way personal data and information were collected by law enforcement agencies. Law enforcement agents conducted stakeouts, pursued sources, and questioned witnesses. Today, many of those investigative functions have been replaced by predictive and prescriptive data analytics.[21] Instead of collecting their own intelligence and data in house, law enforcement agencies outsource data collection and analytics to third-party data brokers and data-as-a-service providers.[22] Data has also become far more prevalent. Until the 1990s, information was largely stored in paper-based filing systems. Crime reports were typed manually or even written by hand. Before that, only the most basic statistical information about crimes and accidents were entered by data clerks into individual law enforcement agency's own, separate mainframe computers.

In the transition from human intelligence to data-based policing methods, police have shifted their power from people to computers, and from internal police files to external software and data vendors. Today, policing agencies don't build their own data troves or investigative schemes. Instead, they outsource their intelligence and surveillance to companies like Palantir,[23] PredPol,[24] and CopLink[25] that develop predictive policing software, and

---

[20] *See, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017); RUHA BENJAMIN, RACE AFTER TECHNOLOGY (2019).

[21] Sarah Brayne, *The Emergence of Big Data Policing*, U. of TEX. AT AUSTIN POPULATION RES. CTR (Aug. 2017), https://repositories.lib.utexas.edu/bitstream/handle/2152/62430/prc-brief-2-11-brayne-policing.pdf [https://perma.cc/AAB4-BDRW].

[22] Data-as-a-service is a term that describes cloud-based software services that warehouse or process data. Some provide data dossiers, some structure the data into information, and some sell data analytics predictions and prescriptions. The companies don't sell data packages outright, rather, they license access to their online data platforms.

[23] *Gotham*, PALANTIR, https://www.palantir.com/platforms/gotham/ (last visited Feb. 7, 2022) [https://perma.cc/K3HS-ZX65].

[24] PREDPOL, https://www.predpol.com/ (last visited Feb. 7, 2022) [https://perma.cc/CL5Z-BYB9].

[25] *Advanced Crime Analytics Platform*, COPLINK, https://forensiclogic.com/coplink/ (last visited Feb. 7, 2022) [https://perma.cc/8DB6-68ZT].

companies like Vigilant[26] and Clearview AI[27] that gather and sell geospatial and biometric data. In order to work, all of these policing products depend on constant flows of data supplied by third-party data brokers.

Data brokers have become de facto primary factfinders in many law enforcement investigations.[28] Predictive policing systems process data supplied by the brokers, and specialized datasets like license plate IDs, DNA markers, and faceprints must be supplemented with data brokers' information-rich dossiers. GPS data alone doesn't do much more than tell someone where you've been, but when you combine GPS data with someone's social media posts, home address, and marriage and criminal records, it's far more revealing.[29] Without data, electronic policing products are empty software and limited pools of designer data. That's why DNA companies,[30] license plate reader companies,[31] predictive policing software companies like Palantir and CopLink[32] partner with data brokers like Oracle, Axciom, RELX and Thomson Reuters. Data is the lifeblood of our datafied policing systems, flowing through all of the algorithms, machine learning, and designer data products, making them work. Third-party data vendors have become such a core part of policing that they've been called *big brother's little helper*.[33]

---

[26] *Vigilant PlateSearch License Plate Recognition Software*, MOTOROLA SOLUTIONS, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/vigilant-platesearch-lpr-analytics-software.html (last visited Feb. 7, 2022) [https://perma.cc/MG6R-HKWX].

[27] CLEARVIEW AI, https://www.clearview.ai/ (last visited Feb. 7, 2022) [https://perma.cc/3BHZ-ACNG].

[28] *See* CENTER FOR DEMOCRACY & TECHNOLOGY, LEGAL LOOPHOLES AND DATA FOR DOLLARS (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf [https://perma.cc/3UWX-4Y66]; *see also* Ferguson, *supra* note 20, at 12–14.

[29] Ian Goldberg, David Wagner & Eric Brewer, *Privacy-Enhancing Technologies for the Internet, in* PROCEEDINGS IEEE COMPCON 103 (IEEE Computer Society ed., 1997).

[30] *See* Adam Stone, *LexisNexis, Bode Technology Team to Accelerate DNA-based Investigations*, WASH. EXEC. (Dec. 16, 2019), https://washingtonexec.com/2019/12/lexisnexis-bode-technology-team-to-accelerate-dna-based-investigations/#.YACST15Om8W [https://perma.cc/KB45-T7D9].

[31] *See* Zack Whittaker, *ICE has a huge license plate database targeting immigrants, documents reveal*, TECHCRUNCH (Mar. 13, 2019), https://techcrunch.com/2019/03/13/ice-license-plates-immigrants/?guccounter=1() [https://perma.cc/SWA8-H23D].

[32] *See Forensic Logic Launches COPLINK X, The Next-Generation Information Network for Law Enforcement*, PR NEWSWIRE (Jul. 16, 2019), https://www.prnewswire.com/news-releases/forensic-logic-launches-coplink-x-the-next-generation-information-network-for-law-enforcement-300885164.html [https://perma.cc/VXG9-ZN59]; *see also Data & Device Partners,* PALANTIR, https://web.archive.org/web/20210128024129/https:/www.palantir.com/partnerships/data-providers/ (last visited May 2, 2022) [https://perma.cc/9V4G-LNLE].

[33] Chris Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595, 595 (2003).

Even though data vendors have become an integral part of U.S. law enforcement, there is little discussion of them in the law. There is not even a settled legal definition for the term "data broker" in federal law. The term has been ascribed to social media companies, consumer reporting agencies, websites that sell peoples' public record data, and to subscription-based "risk" analytics companies.[34] Big tech companies like Amazon and Google are sometimes called first-party data brokers because they share data they get directly from their users.[35] Some data brokers collect specific types of data (like financial or criminal data) or share data in smaller consortia. But there is a cluster of companies sell huge dossiers about all of us to government agencies, including law enforcement agencies.[36] LexisNexis alone supplies data products to 70 percent of local agencies and almost 80 percent of federal agencies to "safeguard citizens,"[37] 2,100 police departments, and 955 sheriff departments.[38] They were paid $16.8 million to provide data services to U.S. Immigration and Customs Enforcement.[39] LexisNexis data services are so embedded in U.S. law enforcement that the company has managed to create a private, third-party fusion center where over 1,300 law enforcement agencies pool and share data beyond the scope of government regulation under the advice of former FBI, Secret Service, and law enforcement officers.[40] These

[34] *See* Justin Sherman, *Federal Privacy Rules Must Get "Data Broker" Definitions Right*, LAWFARE, (April 8, 2021), https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right [https://perma.cc/GFV4-23E9].

[35] *See* Press Release, FTC, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more?utm_source=govdelivery [https://perma.cc/RP32-RYZP].

[36] *See* Wolfie Cristl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*, CRACKED LABS (June 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [https://perma.cc/6GFW-4DYZ].

[37] *Industries We Serve*, LEXISNEXIS, https://www.lexisnexisspecialservices.com/who-we-are/industries/ (last visited Nov. 14, 2021) [https://perma.cc/LT87-PZCT].

[38] ACCURINT, https://www.accurint.com/hr.html (last visited Nov. 11, 2021) [https://perma.cc/A2E9-GP3A].

[39] Sam Biddle, *LexisNexis to Provide Giant Database of Personal Information to ICE*, THE INTERCEPT (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/ [https://perma.cc/TG2K-ZUEG].

[40] The Public Safety Data Exchange (PSDEX) is a contributory database of more than 1,300 law enforcement agencies across the U.S. that was created by LexisNexis Risk Solutions. LexisNexis also claims that its "Accurint Virtual Crime Center" gives law enforcement "greater visibility into crime in both their jurisdictions and nationwide by linking billions of public records with agency-provided data." The Crime Center links to PSDEX and brings together disconnected data to provide a more comprehensive view of people's identities so that law enforcement agencies can better target investigations, identify patterns, predict

third-party data companies have become powerful intelligence apparatus for U.S. law enforcement. Using these third-party data brokers gives law enforcement agencies firehoses dispensing robust flows of personal data, updated in real-time.

IV. THE PRIVACY ACT & THE JETSON EFFECT

The people who drafted the HEW report did a remarkable job of predicting the personal data problems we see today. They knew that the government would become more and more data-dependent, and that government agencies would use data analytics systems to streamline decision making about everything from delivering social security benefits to rooting out cases of fraud. The HEW report even foresaw data processing advancements like predictive analytics and cross-database data sharing.

But neither the experts writing the report or the Privacy Act's drafters were able to predict everything. The Act, like many attempts to guess the future of tech, suffered from the "Jetson Effect"—it predicted some aspects of government data use, but got other key parts wrong. The Jetsons, a 1960-era animated cartoon, depicted the daily life of a family living in the 2000s. While the show correctly guessed some of our technological advances, some of its speculations were mistaken. For example, the show correctly predicted that we'd converse by video chat, watch flat screen TVs, and wear smartwatches on our wrists, but it wrongly assumed that we'd replace our street vehicles with flying cars and that our technology would rely on cogs and sprockets instead of tiny microchips.

In the Privacy Act, 1970s-era policymakers tried to regulate the future of the federal government's data practices in the same way Jetsons writers guessed at the future of family life in the 2000s. Congress tried to envision the future of government data systems, and the law was thus limited by the imaginations of its creators.[41] Despite their efforts, the Privacy Act's drafters did not envision today's data broker landscape. The law correctly assumes that the government might try to use personal data in secret programs, and that without limits, the government data programs may suffer from "mission creep,"

---

upcoming events and deploy resources more efficiently. *Prevent and Solve More Crimes with Data-Driven Insights*, LEXISNEXIS, https://risk.lexisnexis.com/law-enforcement-and-public-safety/information-data-sharing (last visited Apr. 25, 2022) [https://perma.cc/S9V6-JPUQ].

[41] U.S. DEP'T OF JUST., *supra* note 13. ("In the more than 45 years since the Privacy Act was enacted, information technologies have expanded in ways that the drafters of the HEW Report could never have imagined, and the risks associated with the collection and use of personal data have grown accordingly.").

where data collections are used beyond their intended purposes.[42] But the Privacy Act erroneously assumes that the government will collect its own data and store and manage that data internally.

The law's drafters envisioned a system where federal agencies collect, organize, and maintain our data. At the time the law was passed, the government was not purchasing data, but building its own data collections. It's not surprising, given the lack of a data brokering industry in 1974, that the HEW report describes how Congress should balance the mutual interests of government institutions and individuals, but it does not include the interests of third-party data brokers.[43] The law does not cover the current reality, where data brokers do the work of collecting, maintaining, and organizing government's personal data programs.

Instead, the Privacy Act only applies to the federal government's data systems and to private companies that administer those government systems.[44] When government information is transferred to a private company, the Privacy Act requirements apply to that contractor. But when a privacy company collects or creates its own data, those data collections are beyond the Privacy Act's scope.[45] For instance, if the U.S. Marshals Service (USMS) creates its own database containing fugitives' data, it must follow the Privacy Act's requirements.[46] But if the USMS uses a data broker instead, the Privacy Act does not apply.[47] Once a government agency integrates data brokers' data into its own systems of records, the Privacy Act may apply, but, especially with law enforcement records, there are other Privacy Act provisions that limit the public's access and correction rights to those files.[48]

---

[42] Mission creep is a term that was originally used to describe the gradual shift in objectives that happens in some government operations, like the U.S. deployment of troops to Somalia in the 1990s. The troops were sent to protect relief agencies as they distributed food, but after they arrived, their mission became a fighting mission far beyond the scope of what was initially intended. The government's use of commercial sources of information in surveillance is especially vulnerable to mission creep. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1492 (2004).

[43] *HEW Report*, *supra* note 3, at 52.

[44] 5 U.S.C. § 552a(m)(1)-(2). ("When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.").

[45] Moreover, "consumer reporting agencies" are explicitly exempted from the Privacy Act's requirements. 5 U.S.C. § 552a(m)(1)-(2) ("A consumer reporting agency to which a record is disclosed under section 3711(e) of Title 31 shall not be considered a contractor for the purposes of this section"); *see* Hoofnagle, *supra* note 33, at 623.

[46] 5 U.S.C. § 552a; Hoofnagle, *supra* note 33, at 633.

[47] Hoofnagle, *supra* note 33, at 633.

[48] 5 U.S.C. § 552a(j)-(k).

The Privacy Act also assumes that our personal datasets would remain in separate, siloed data systems. In the 1970s, our internet system was not fully formed and data was kept in mainframe computers that did not communicate. Each system carried different records. Some held administrative records (i.e., marriage licenses, work permits), some held intelligence records (i.e., police investigation files, security clearance files, consumer credit reports), but the siloes could not easily be combined.[49] The drafters did not envision a world where data companies could instantaneously pull and combine data from over 10,000 sources and apply that data across various analytics programs.[50]

The Act also exempts broad categories of data based on the political and social status quo in 1974. For example, when Congress passed the Privacy Act, it chose to exempt criminal investigation records from many of the law's transparency provisions.[51] This exemption for law enforcement records reflects similar policy choices made in other federal records laws during same this same era. In the 1970s, Congress included broad national security and police records exemptions in all information laws. Laws from the Freedom of Information Act to the Presidential Records Act made clear that law enforcement was to be kept out of the public's view.[52] Because these laws did not anticipate the sprawling data surveillance schemes and big data policing as they exist today, they did not make exceptions for transparency so that we could learn how law enforcement and intelligence agencies are using our data.

It is likely that political calculations in favor of law enforcement, as well as a focus on the way data was being used by the government in the 1970s, paved the way for these law enforcement and other surveillance carve-outs in the law. At the time of the report, data systems were already being used to determine and track social welfare transactions and Social Security numbers, not policing. The geospatial and biometric data tools police are swarming to use, as well as the predictive policing data products that companies are making today, did not even exist then. It was the stuff of science fiction.[53]

The Privacy Act provisions limiting the law's application to law enforcement and data brokers' data streams do not align with the ways the federal government obtains and uses our data in the 21st Century. Today, law

---

[49] *See HEW Report*, *supra* note 3, at 5-6.

[50] LexisNexis is just one data broker that sells access to millions of personal data dossiers that combine data from thousands of sources. *See* James Burton, *LexID Linking Technology: What Is It and What Does It Do?*, LEXISNEXIS RISK SOLUTIONS (Nov. 4, 2016), https://blogs.lexisnexis.com/insurance-insights/2016/11/lexid-linking-technology-what-is-it-and-what-does-it-do/ [https://perma.cc/MP6V-3YJ7].

[51] 5 U.S.C. § 552a(j)(2).

[52] *HEW Report*, *supra* note 3, at 35.

[53] These types of policing systems were described in Philip K. Dick's 1956 sci-fi novella, Minority Report. Philip K. Dick, *The Minority Report*, FANTASTIC UNIVERSE, Jan. 1956, at 4.

enforcement and other government agencies license data brokers' products instead of purchasing ownership rights to the data they need. Then, law enforcement agents access the data products on third-party platforms instead of in locally-hosted data systems. Data brokers stream our personal data dossiers from data clouds beyond the government's files. The third-party data dossiers give the government our public records information (license data, criminal history, etc.), and they also provide law enforcement with our consumer data, social media activity, warranty registrations, magazine subscriptions, religious and political affiliations, and other details about our daily lives.[54]

Another thing the Privacy Act's drafters did not anticipate was the value of data as capital in the 2000s. Data has become more than a useful tool for public and private institutions: it is a lucrative resource to buy and sell. Because data fuels so many digital devices and systems, public institutions that generate public records—including arrest records, land sale recordings, and data rolls from Departments of Motor Vehicles (DMVs)—sell that data to brokers and other third parties for profit.[55] As summarized by a Washington State employee, the DMV is not just a public-safety agency but "very much a data-sharing agency."[56] In the reverse, data brokers solicit data from law enforcement, building more and more data products to license to them on their platforms.[57] Data brokers even send their own employees to help agents use their data services, sitting side-by-side with law enforcement customers.[58] The

[54] Doug Wyllie, *New LexisNexis Service Keeps Tabs on Social Media*, POLICE1 BY LEXIPOL (Jan. 30, 2014), https://www.police1.com/police-products/investigation/investigative-software/articles/new-lexisnexis-service-keeps-tabs-on-social-media-KfCucEkc3UnXtP5Z/ [https://perma.cc/CS2G-4WWA].

[55] Hoofnagle, *supra* note 33, at 624.

[56] Some government agencies sell our personal data to bolster state budgets. In 2017 alone, Washington State's Department of Licensing made $26,371,232 selling driver and vehicle records to data brokers, including LexisNexis and companies that work with Thomson Reuters. McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/Q9XQ-BH54].

[57] Hoofnagle, *supra* note 33, at 599; Sam Biddle & Spencer Woodman, *These Are the Technology Firms Lining Up to Build Trump's "Extreme Vetting" Program*, THE INTERCEPT (Aug. 7, 2017), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ [https://perma.cc/XT5Y-NSRG] (reporting that the "Technology Firms" included data brokers like LexisNexis, who attended to learn more about what kinds of data services ICE needed).

[58] Hannah Beckler, *Thomson Reuters Analysts Process Data to Help ICE Agents Make Arrests, Documents Show*, DOCUMENTED (May 20, 2020), https://documentedny.com/2020/05/20/thomson-reuters-analysts-process-data-to-help-ice-agents-make-arrests-documents-show/ [https://perma.cc/Y8JY-HBPM].

best place to get public government records isn't from the government itself, but from private companies like Oracle and RELX.

V. THE JETSONS EFFECT IN LAW ENFORCEMENT: ICE'S THIRD-PARTY DATA POLICING INFRASTRUCTURE

The Privacy Act carves out broad exemptions for data involved in criminal investigations even though today, the agencies that most need Privacy Act-styled safeguards are law enforcement agencies. Law enforcement agencies are uniquely able to use personal data to interfere with people's rights and liberties. Law enforcement agents can use data systems to track us, to make decisions about whether to detain us, and to put us before tribunals that can imprison us, deport us, and even sentence us to death. While the general problems of bias and erroneous decision-making in policing have remained consistent, policing itself, as an activity, has evolved over the past 48 years. One federal policing entity puts these changes on stark display: the Immigration and Customs Enforcement (ICE). ICE is building massive surveillance and big data policing infrastructure with third party software and data, so it is beyond the scope of information laws like the Privacy Act.[59]

ICE's data-powered surveillance and data dragnets make immigration raids scenes that could be described in a dystopian novel.[60] ICE detained a 10-

---

[59] Mijente & National Immigration Project 2018, *Who's Behind ICE: The Tech and Data Companies Fueling Deportations*, IMMIGRANT DEFENSE PROJECT (Aug. 23, 2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf [https://perma.cc/9PRM-SRSD].

[60] *See* Daniel Oberhaus, *ICE Modified its "Risk Assessment" Software So It Automatically Recommends Detention*, MOTHERBOARD (June 26, 2018), https://motherboard.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention [https://perma.cc/5BHK-6FAK] (reporting on new settings in ICE's Risk Classification Assessment program which now automatically recommends detention conforming to Trump's "zero tolerance" stance and leads to an increase in the detention of people with little or no criminal history); Nick Miroff & Maria Sacchetti, *Trump Takes "Shackles" Off ICE, Which is Slapping Them on Immigrants Who Thought They Were Safe*, WASH. POST (Feb. 11, 2018), https://www.washingtonpost.com/world/national-security/trump-takes-shackles-off-ice-which-is-slapping-them-on-immigrants-who-thought-they-were-safe/2018/02/11/4bd5c164-083a-11e8-b48c-b07fea957bd5_story.html?utm_term=.f6ef0b26d0dc [https://perma.cc/KM6Z-8373] (reporting that ICE arrests have surged 40% under the Trump administration, and claiming that ICE made 37,734 "noncriminal" arrests in the 2017 fiscal year, more than twice the number from the previous year); Caitlin Dickerson, *Immigration Arrests Rise Sharply as a Trump Mandate is Carried Out*, N.Y. TIMES (May 17, 2017), https://www.nytimes.com/2017/05/17/us/immigration-enforcement-ice-arrests.html [https://perma.cc/JC77-M6WS] (The mandate referred to in the title is the rescinding of Obama era rules that prioritized arrests of "serious criminals," rather than applying ICE enforcement across all undocumented populations, regardless of the seriousness of crimes, opening enforcement to people committing minor infractions and

year-old girl with cerebral palsy immediately after she had surgery. She had lived in the United States since she was three months old, and agents tracked and located her at 2 a.m. as an ambulance transported her between hospitals.[61] In New York, ICE agents arrested a high school student hours before his senior prom;[62] a couple visiting their son-in-law; and a sergeant in the U.S. Army on the Fourth of July[63]—just to name a few. Comprehensive personal data dossiers, updated in real time, containing geolocation and biometric data, make ICE raids swift and surprising, catching people off guard in vulnerable moments. As one teacher whose students' parents were taken by ICE agents described it: "One moment they're living life ... and then they're gone, their car just sitting on the side of the road. It feels like a death."[64]

The most common questions among immigrants at the receiving end of ICE arrests and raids are "*How did they pick me as a target?*" and "*How did they find me?*"[65] The answers to these questions can often be found in subjects' data dossiers. Data analytics companies' products "form an ever-evolving, 360-degree view" of ICE subjects' lives by supplying information about workplaces, locations, associates, affiliations, etc. ICE agents use this information to make hot lists and heat maps that tell the agents whom to track and where to find them without any regulatory safeguards.[66]

misdemeanors); *see* Memorandum from John Kelly, Secretary, Department of Homeland Security (Feb. 20, 2017), https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Enforcement-of-the-Immigration-Laws-to-Serve-the-National-Interest.pdf [https://perma.cc/Y6TA-Y955] (mandating changes in immigration enforcement priorities).

[61] Lia Eustachewich, *Girl with Cerebral Palsy Detained by Immigration Agents After Surgery*, N.Y. POST (Oct. 26, 2017), https://nypost.com/2017/10/26/girl-with-cerebral-palsy-detained-by-ice-agents-after-surgery/ [https://perma.cc/YT86-FYAX].

[62] Michael P. McKinney & Jorge Fitz-Gibbon, *ICE Agents Arrest High Schooler Hours Before Prom*, USA TODAY (June 9, 2017), https://www.usatoday.com/story/news/nation-now/2017/06/09/high-school-student-immigration-arrest/385457001/ [https://perma.cc/JA7J-YUQ7].

[63] Samantha Schmidt, *A Couple Visited Their Soldier Son-In-Law on July 4. The Army Turned Them Over to ICE.*, WASH. POST (July 10, 201), https://www.washingtonpost.com/news/morning-mix/wp/2018/07/10/a-couple-visited-their-soldier-son-in-law-on-july-4-the-army-turned-them-over-to-ice/?noredirect=on&utm_term=.322e768c6639 [https://perma.cc/635A-586T].

[64] Funk, *supra* note 56.

[65] Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, WASH. POST (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/ [https://perma.cc/E2ZF-RBPV].

[66] Funk, *supra* note 56.

VI. DATA BROKER EXEMPTIONS PERMIT THE PROBLEMS THE PRIVACY ACT WAS MEANT TO PREVENT

The Privacy Act has been updated a few times in the past fifty years,[67] but no amendment has contemplated third-party data brokers, even as law enforcement agencies like ICE expand their personal data use in ways that violate personal privacy and due process. A fully implemented Privacy Act that includes data brokers in its scope could address the major problems that data broker-powered policing causes, including providing due process, increasing transparency, preventing mission creep, and reducing bias in the government's data-driven policing programs.

A. Privacy Act provides due process

The Privacy Act provides much needed due process in the government's use of our personal data. Since the Supreme Court excluded third-party data from the Fourth Amendment's warrant requirements, [68] government agencies have been able to "buy their way around" the obligation to show probable cause to search our records.[69] The third-party doctrine was developed around the same time the Privacy Act became law, long before big data policing developed into a third-party-run infrastructure. The doctrine assumes that people give their information to third parties voluntarily, knowingly, and consensually, like a businessperson giving their records to an accountant or someone describing a crime to an informant. But the doctrine is outmoded by current policing practices, which rely on data we did not knowingly or consensually share.[70] Because data brokers are not required to obtain warrants or subpoenas before they collect, search, and share personal

---

[67] *See, e.g.*, The Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503; *see, e.g.*, The Computer Matching and Privacy Protection Amendments of 1990, Pub. L. 101-508.

[68] Third-party doctrine was established in United States v. Miller, 425 U.S. 435 (1976). Even though the doctrine has been narrowed a bit by cases like Carpenter v. United States, 585 U.S. ___ (2018), the third-party doctrine still excludes most third-party data from the Fourth Amendment's warrant requirements. *See* United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (holding that the third-party doctrine applies to information on the Bitcoin blockchain by comparing such information to bank records which are subject to the Fourth Amendment exception).

[69] Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment*?, WIRED (Feb. 11, 2020), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/ [https://perma.cc/6QNG-J9SW].

[70] United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, S., concurring) (calling the warrant exception "ill-suited to the digital age"); Carpenter v. U.S., 585 U.S. ___ (2018); 138 S. Ct. 2206; 201 L. Ed. 2d 507 (exempting cell phone location data from the third-party doctrine).

data, they can advertise their services as ones that have "no need for a court order."[71]

The Privacy Act does not add warrant requirements for government data collections, but it does guarantee that people have some procedural due process before agencies can collect and use your data. Specifically, the Privacy Act requires that the public be given notice and have the opportunity to comment on any new "systems of records" that federal agencies collect.[72] It also gives individuals the right to obtain their own information and learn how and why it is being used in a system of records.[73] These procedural mechanisms were meant to ensure that the government was not obtaining and searching people's data in secret nor using individuals' data without their knowledge or consent. Policymakers also intended to prevent government agencies from using personal data in dragnet policing schemes where, instead of focusing on suspects, law enforcement would sift through personal data to create suspects using data analytics software.[74] The law even requires agencies to collect information directly from individuals instead of relying on databases "to the greatest extent possible" when the information may result in adverse determinations about the individual's rights or privileges.[75]

The 1970s-era policymakers' fears about secret, dragnet policing programs proved true. Without robust Privacy Act-like procedures in place, the government implemented invasive data surveillance and targeting schemes to track people in the wake of 9/11.[76] Since little was done to prevent data surveillance, even after Edward Snowden's 2013 revelations about phone and internet data surveillance, dragnet-style data policing practices have expanded into other law enforcement systems, including child welfare, financial crimes

---

[71] Hoofnagle, *supra* note 33, at 621 (quoting eBay's director of Law Enforcement and Compliance Department regarding how the company was framing its privacy policy to cater to law enforcement searches).

[72] 5 U.S.C. § 522a(e).

[73] 5 U.S.C. § 552a(e)(3).

[74] Arlen J. Large, *Congress Finishes Work on 'Privacy' Bill But Measure Has a Number of Loopholes*, *in* SOURCE BOOK, 1237 (1976). People were concerned that universal identifiers like social security numbers would become the basis for "master files" where the government gathers our data into massive dossiers comprised of merged, unrelated files that would be used across agencies and in various data analytics schemes and used to match people based on various data points. *See HEW Report*, *supra* note 3, at 20.

[75] 5 U.S.C. § 552a(e)(2).

[76] Edward Snowden, *NSA Surveillance Exposed by Snowden Was Illegal, Court Rules Seven Years On*, GUARDIAN (Sept. 3, 2020), https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules [https://perma.cc/V68Q-X3LW]. This post-9/11 dragnet policing was the historical backdrop for Hoofnagle's article raising concerns about data brokers and the government's use of third-party data dossiers. Hoofnagle, *supra* note 33, at 621.

enforcement, and even tax evasion.[77] The U.S. Postal Service even tracks our social media posts to "assess[] threats to Postal Service employees and its infrastructure."[78]

The expansion of data policing programs makes due process provisions—such as the provisions found in the Privacy Act—more important than ever. Today's law enforcement data brokers assign universal identifiers to all of us, gathering billions of datapoints from over 10,000 sources to our identifier and updating those datapoints in real time.[79] With third-party data brokers' data-streaming services, law enforcement can combine different datasets to create mosaics of our lives: where we go, who we know, and what we do each day.[80] Even if you try to opt out of data collection by avoiding social media, the companies create "shadow profiles" about you based on the data your friends, family, and associates trail behind them when they go online.[81] If you try to remove your online data, companies like Thomson Reuters can make you reappear, from "invisible to stark visibility."[82] Data brokers don't just sell peoples' data, they also sell predictions (*Who will commit a crime?*) and prescriptions (*Track this person.*) for governments and companies to follow.[83] Data analytics products like these make due process a paramount concern for a public that is subjected to the products' computerized decisions about surveillance and arrests without any notice or way to dispute the data-based decisions.

---

[77] Christopher M. Ferguson, *The IRS's Big Plans for Big Data*, CPA J. (Oct. 26, 2021), https://www.cpajournal.com/2021/10/26/the-irss-big-plans-for-big-data/ [https://perma.cc/3M4A-G2Z2].

[78] EPIC v. U.S. Postal Service et. al, No. 21-2156 (D.D.C. filed Aug. 12, 2021).

[79] RELX calls theirs "LexIDs," and the company uses its "linking technology" to enrich our IDs with data and connections. LexisNexis Risk Solutions, https://blogs.lexisnexis.com/insurance-insights/2016/11/lexid-linking-technology-what-is-it-and-what-does-it-do/ (last visited on Feb. 7, 2022) [https://perma.cc/DTY3-ALEV].

[80] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L. J. 628, 628–79 (2005).

[81] Andrew Quodling, *Shadow Profiles - Facebook Knows About You, Even if You're Not on Facebook*, CONVERSATION (Apr. 13, 2018, 2:41 AM), https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804 [https://perma.cc/M2K3-XZXS].

[82] *What Investigators Can Learn From People Who Want to Disappear*, Thomson Reuters (Dec. 3, 2019), https://legal.thomsonreuters.com/blog/what-investigators-can-learn-from-people-who-want-to-disappear/ [https://perma.cc/4YGF-JGV5].

[83] Liam Kane, *Agile Data Science — Part 2*, BURNDOWN (Oct. 28, 2017), https://theburndown.com/2017/10/28/agile-data-science-part-2/ [https://perma.cc/6CJC-4X7E].

B. Privacy Act creates transparency

In addition to ensuring that people have notice of, and the opportunity to comment on, government data programs, the Privacy Act also makes government data programs more transparent. When agencies create a new system of records, or amend an old system of records, they must notify the public of those changes with in-depth "Systems of Records Notices" (SORNs). Notice requirements force agencies to provide the name and location of data systems; descriptions of the individuals whose records are contained in each system and the types of records that are being collected; the purpose of the collection and an explanation of how the records will be used; the storage, retrieval, access, retention and disposal practices for the collection; the title and address of the agency official responsible for the system of records; the agency procedures for getting access to records; and information about the sources for the records in the system.[84]

As data brokers are not treated as subjects of the Privacy Act, the companies do not provide any of this information. This lack of transparency makes it hard to figure out exactly how the government uses data analytics products and exactly what the products contain. Immigration rights advocates and criminal justice groups spend thousands of dollars and hundreds of hours filing FOIA requests and suing agencies that fail to comply with the transparency law.[85]

When the public is able to wrest a few meager records about data broker deals from government agencies, it is nearly impossible to parse the information in those records[86] to figure out who is accessing the data services and what they are using them for. The obscurity in those records seems intentional. Like other personal data licensing agreements, data brokers' contracts with customers are notoriously hard to make sense of; they seem almost "purposefully dense and dull."[87] Some experts suspect that the

---

[84] 5 U.S.C. § 552a (e)(4)(A)-(I).

[85] *See, e.g.*, Just Futures Law v. U.S. Dep't of Homeland Security, 1:21-cv-02208 (D.C. Cir. filed Aug. 19, 2021) (suing Dep't of Homeland Security to obtain LexisNexis contract records); *see, e.g.*, N.Y. Times v. U.S. Dep't of Defense, 1:21-cv-10980 (S.D.N.Y filed Dec. 22, 2021) (suing Defense Intelligence Agency for documents that would show whether it has been purchasing Domain Name System (DNS) logs or Internet traffic data from commercial brokers).

[86] Usually the only information we can get about how law enforcement agencies use data brokers is what we can cobble together from contracts we wrest from the agencies via FOIA or the rare Privacy Impact Assessment that an agency may prepare regarding programs that use personally identifiable information.

[87] Charlie Warzel, *The Internet's Original Sin: Shoshana Wodinsky Explains Bad Ads*, GALAXY BRAIN (Sept. 23, 2021), https://warzel.substack.com/p/the-internets-original-sin?s=r [https://perma.cc/NRS7-7XPN].

companies and institutions involved make "the most interesting stuff . . . the most impenetrable" to prevent the public from discovering just how our personal information is being used by powerful decision-making entities.[88]

C. Privacy Act prevents mission creep

The Privacy Act also contains provisions that prevent personal data from being used beyond its intended, routine purpose. In the 1970s, senators were concerned that a glut of personal data, without restrictions on use or maintenance, "creates a temptation to use [the data] for improper purposes."[89] The Act requires that agencies maintain only information relevant and necessary for a purpose required to be accomplished by law.[90] Agencies must also explain how they will store, retrieve, retain, and dispose of records for each system of records they create and describe who will have access to the records.[91] Finally, agencies have to establish "appropriate administrative, technical, and physical safeguards" to insure the security and confidentiality of our records and to prevent the records from being misused to harm us.[92] While these types of provisions do not create a perfect level of protection against mission creep, they do help prevent data from being misused or treated like a trove to save for future use, even after its intended purpose is completed.

The Privacy Act makes clear that our personal data is not meant to be a goldmine that gets stored away for future use. It is meant to be ephemeral. Government data collections should solve a specific problem, and then go away. The HEW report authors advised Privacy Act drafters to ensure that data only be transferred under controlled conditions, to prevent blurring the lines between types of records and intended uses.[93] The authors also advised the to limit data collection by recording "only information that has a clear-cut relevance to its concerns."[94] The data management provisions in the Privacy Act carry out these goals.

But because the Privacy Act's data management requirements are not applied to the government's data brokers, mission creep pervades law enforcement agencies' data practices. In San Diego, data from smart streetlight cameras installed to solve violent attacks is instead used to arrest people for

---

[88] *Id.*
[89] SELECT COMM. TO STUDY GOV'TAL OPERATIONS WITH RESPECT TO INTEL. ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPS. ON INTEL.ACTIVITIES & THE RTS. OF AMS., S. REP. NO. 94-755, at 778 (2d Sess. 1976).
[90] 5 U.S.C. § 552a(e)(1).
[91] *Id.* at § 552a(e)(4)(E).
[92] *Id.* at § 552a(e)(10).
[93] HEW REPORT, *supra* note 3, at 7.
[94] *Id.* at 6.

minor crimes like illegal dumping and vandalism.[95] In New York City, video recorded by digital kiosks was purposely kept separate from the New York Police Department's camera system until someone started smashing the kiosks. Then, the footage was sent to police for use in law enforcement.[96]

Individual law enforcement officers also use data brokers' products beyond their intended purposes. When law enforcement agents misuse their physical weapons, they face consequences like disciplinary actions, dismissal, and lawsuits.[97] But there are no consequences when police officers misuse data broker subscriptions. In most cases, officers' use of third-party personal data products is not monitored.[98] When the FBI subscribed to ChoicePoint in the 1990s, agency employees were encouraged to "use ChoicePoint to [their] heart's[']content."[99] Without oversight, law enforcement officers use data brokers' products however they want, even if the use is beyond the purpose of the data program,[100] and agencies do not have to expunge data after the program's intended purpose is accomplished.[101]

D. Privacy Act makes the government correct erroneous data

The Privacy Act requires agencies to maintain accurate records and correct erroneous facts.[102] While the Privacy Act does not account for algorithmic biases that are pervasive in predictive policing and other personal

---

[95] Jesse Marx, *The Mission Creep of Smart Streetlights*, VOICE OF SAN DIEGO (Feb. 3, 2020), https://www.voiceofsandiego.org/topics/public-safety/the-mission-creep-of-smart-streetlights/ [https://perma.cc/2WUZ-Q3W4].

[96] Claire Lampen, *Yes, LinkNYC Kiosks Are Giant Data-Harvesting Surveillance Cameras, Obviously*, GOTHAMIST (Apr. 25, 2019), https://gothamist.com/news/yes-linknyc-kiosks-are-giant-data-harvesting-surveillance-cameras-obviously [https://perma.cc/APJ6-9KU5]; *see also* Annie McDonough, *How New York City is Watching You,* CITY & STATE NEW YORK (Apr. 29, 2019), https://www.cityandstateny.com/articles/policy/technology/how-new-york-city-is-watching-you.html [https://perma.cc/4BJ5-EY84].

[97] *See* Hoofnagle, *supra* note 33, at 595.

[98] *Id.* at 599.

[99] *Id.* at 619.

[100] Sadie Gurman, *Across US, police officers abuse confidential databases*, ASSOC. PRESS, (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43 [https://perma.cc/Q5Z7-2SCU].

[101] Unlike Europol, which had to expunge data it kept too long in violation of EU data protection laws, data brokers in the U.S. never have to expunge data. Apostolis Fotiadis, Ludek Stavinoha, Giacomo Zandonini, & Daniel Howden, *A data 'black hole': Europol ordered to delete vast store of personal data*, GUARDIAN, (Jan. 10, 2022), https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data [https://perma.cc/KN82-CATC].

[102] 5 U.S.C. § 552a(e)(5), (d)(2)(B)(i).

data-sorting software,[103] or repair the bias caused by the overrepresentation of over-criminalized people (and especially Black men) in law enforcement datasets,[104] fixing personal data errors does offer some redress and quality control in the government's data collections.

Data brokers do not do the same kind of quality control in their data collections, nor do they let people fix errors in their records, even when they sell those records to government agencies. And data brokers' records contain plenty of errors, including accidentally swapping the data of individuals with the same names. With thousands of unique data sources and billions of pieces of data, the main data brokers that work with law enforcement can hardly fact-check every bit of data they send to law enforcement. Instead of vetting their data dossiers, data brokers tell consumers that if they want to fix data errors, they must contact the downstream data providers. Figuring out the source of the erroneous data and requesting that source amend its datasets is a nearly impossible task. Even if a person manages to amend the incorrect data, they

---

[103] *See, e.g.*, SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); RUHA BENJAMIN, RACE AFTER TECHNOLOGY (2019).

[104] The impacts of historic systemic racism that blocked Black people from amassing financial savings, obtaining housing, and enjoying the fruits of economic benefits also mean that they have more of their personal data in digital systems that manage social services programs. When data analytics companies use this data in their government products, it results in disparate treatment. For instance, the disparate data dossiers make Black children the focus of child welfare algorithms, which makes Black children more likely to be tracked and their families disparately subjected to state intervention. Elizabeth Brico, *When Data Discriminates*, MEDIUM (Apr. 17, 2019), https://medium.com/the-ai-issue-weapons-of-reason/when-data-discriminates-4791f14c5906 [https://perma.cc/GSU7-388E]. The Chicago Police Department's failed "Strategic Subjects List" program used a computerized algorithm to rank people's likelihood of committing a crime and did not reduce gun violence, which resulted in disproportionate police contact with people who appeared more on the lists. People with more data in the system showed up more prominently in the system and they subsequently had more police interactions that created even more data in their files. Jessica Saunders, *Predictions Put Into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, J. EXPERIMENTAL CRIMINOLOGY 12, 347–71 (2016), https://doi.org/10.1007/s11292-016-9272-0; [https://perma.cc/GR68-KV8K] Jeremy Gorner & Annie Sweeney, *For Years Chicago Police Rated the Risk of Tens of Thousands Being Caught Up in Violence. That Controversial Effort has been Quietly Ended*, CHICAGO TRIBUNE, (Jan. 24, 2020), https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html [https://perma.cc/EDX2-96UJ]. Similarly, undocumented immigrants are more likely to be tracked by immigration enforcement the more they comply with U.S. laws, generating digital "paper trails" by getting licenses and insurance, paying bills, sending kids to school, filing taxes, working, and participating in society. Social participation makes people more "findable." The U.S. government encourages immigrants to assimilate, applauding people who perform "model citizenship," but builds systems where people who follow government rules have thick data dossiers that are weaponized by law enforcement. Funk, *supra* note 56.

can only hope that the fixed data filters upwards to the major data broker selling the data to the government.[105] This is a lousy process for fixing errors that could lead to mistaken surveillance, arrest, and even detention.

VII. BREATHING NEW LIFE INTO THE OLD PRIVACY ACT

We do not need an entirely new law to address governmental data use. As law professor and data law expert Chris Hoofnagle concluded at the end of his 2004 article on data brokers and law enforcement, "[t]he Privacy Act of 1974 should apply to [Commercial Data Brokers]."[106] We can start solving some of the privacy problems and injustices inherent in big data policing by simply implementing the Privacy Act in the way it was intended—making sure that the government's data brokers and law enforcement agencies are bound by its requirements, and that the law's provisions are given their full force by regulators and courts.

We can also amend the law to account for big data policing and government data brokering. The Privacy Act can be a vehicle not just for correcting individuals' data files, but also for remedying biased datasets, algorithms, machine learning, and AI software. If data systems are found to risk the formulation of biased and erroneous law enforcement decisions, they should not be used. While the Privacy Act will not solve all data injustice problems, it could be a tool to alleviate some issues while we design better overarching data rules and infrastructure. We desperately need to change our approach to big tech as a nation and to revisit everything from antitrust laws to copyright schemes to make U.S. law comport with the realities of our modern data realities. Bringing our records law in line with big tech reality is one part of that necessary change.

---

[105] *See* Shea Swauger, (@SheaSwauger), TWITTER (Dec. 13, 2019, 3:53 PM), https://twitter.com/SheaSwauger/status/1205591704973103104 [https://perma.cc/WX2V-SWB9].

[106] Hoofnagle, *supra* note 33, at 629.