LOGIN.GOV AND THE UNCERTAIN EARLY LIFE OF AMERICA'S NATIONAL DIGITAL ID

Talya R. Nevins*

Login.gov is America's new nationwide Digital ID system. In its few years of existence, it is already the only way to access an increasing number of government programs, benefits, and resources. The significance of this development hides behind technical details, confidential contracts, and jargony hyphenates like "single-sign-on" and "duo-authentication." Yet properly examined, the story of why Login.gov was created, with whose input, and with which governance goals in mind exposes both the promise and pitfalls of infrastructural projects in the digital age.

A central facet of the Login.gov infrastructure is its reliance on a notoriously extractive and inscrutable data broker, LexisNexis. LexisNexis verifies the identities of Login.gov users—often welfare applicants, veterans, and federal employees—by comparing data input by users to a vast array of records scraped from every nook and cranny of the internet. The government's decision to partner with LexisNexis openly flouted binding privacy and security guidelines set by the government's own science and technology experts. Moreover, this massive aggregation of personal information, though legal, goes against the best practices for government collection and use of personal data set forth in the Privacy Act of 1974.

As ineffective as the Privacy Act of 1974 is as a data privacy law in the age of online data brokers, the law nevertheless represents a substantial effort by legislators from a bygone era to set principled guidelines for how to build trustworthy, democratically sustainable information systems. By contrast, the early years of America's first nationwide digital identity credential are characterized by unscrupulous design judgments with dangerous consequences. But it is not too late to design tomorrow's digital infrastructure to be safer, more equitable, and more trustworthy than what we have today.

* Copyright © 2024 by Talya R. Nevins, J.D., 2024, New York University School of Law. I am grateful to Professor Benedict Kingsbury for his critical guidance throughout the development of this Note. I also thank Professors Thomas Streinz, David Stein, Angelina Fisher, and Victoria Adelmant for their essential comments, feedback, and suggestions. I also owe deep thanks to Taylor Riddick for her thoughtful edits as the Primary Editor on this Note; Daniel Kenny, Apurva Panse, Eunice Park, Leila Murphy, Grant Welby, Bhavini Kakani, Adam Revello, Isabel Paolini, and Ben Perelmuter for the early-stage feedback; and other members of the *New York University Law Review* who worked on this piece.

Introduction

In 2017, the federal government began rolling out Login.gov, a single-sign-on portal for access to government resources online. The idea is for each person in the United States to create a username and password with Login.gov, which she can then use any time she wants to interact with the government online. Instead of creating one account to file taxes with the Internal Revenue Service (IRS), another to register for unemployment benefits from the Department of Labor, and another to access healthcare through the Department of Veterans Affairs, a person's Login.gov account will suffice to access all these agencies' websites. Its stated purpose is to serve as "[t]he public's one account for government."[1]

As anyone who has struggled to keep track of their passwords will understand, a single-sign-on system is attractively simple for

[1] Login.gov, https://login.gov [https://perma.cc/L9E5-HM7K].

users. And an all-access sign-on platform is more cost-effective for the government than a system where each agency must create and maintain a sufficiently reliable login system. But this alluringly simple and efficient infrastructure carries monumental implications for how the federal government collects, secures, maintains, and uses information about us. And based on that information, Login.gov algorithmically mediates who can access government resources, and who will be denied. The technical design choices made in its early life thus constitute the future of governance, for better or for worse.

Building functional, trustworthy, and efficient civic technology is a worthy goal in an increasingly digital world. But if implemented improperly, modern society risks "stumbling zombie-like into a digital welfare dystopia."[2] Countries around the world are building Digital ID systems that use digital technologies to establish and authenticate individuals' unique identities remotely, over the internet. Like Login.gov, these systems generally have the stated aim of expanding access to government resources.[3] But human rights advocates have shown how, perversely, Digital ID systems often surveil, exclude, and discriminate against vulnerable groups.[4] Already powerful actors like international organizations, technology vendors, and consultants are overrepresented in the design of Digital ID systems, and tend to be the clearest beneficiaries of Digital ID.[5] Unless a Digital ID system is designed according to democratic community input, it is unlikely to serve a given constituency's needs. But this is not how Login.gov was built.

The U.S. government doesn't call Login.gov "Digital ID," but that is what it is. Login.gov is a new, nationwide digital identification

[2] Philip Alston (Special Rapporteur on Extreme Poverty and Human Rights), *Report of the Special Rapporteur on Extreme Poverty and Human Rights*, ¶ 72, Gen. Assembly, U.N. Doc. A/74/48037 (Oct. 11, 2019), https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx [https://perma.cc/2J53-M8SL].

[3] *See* Ctr. Hum. Rts. & Glob. Just., Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID 13 (2022), https://chrgj.org/2022-06-paving-digital-road-to-hell [https://perma.cc/WP5K-EKBK].

[4] *See id.* at 8; *see also* Sara Baker, *Digital ID: A Primer*, *in* Resisting Borders and Technologies of Violence 115 (Mizue Aizeki, Matt Mahmoudi & Coline Schupfer eds., 2024) (presenting key arguments for and against Digital ID and highlighting the danger of massive data collection for already marginalized and surveilled communities).

[5] *See* Ctr. Hum. Rts. & Glob. Just., *supra* note 3, at 8–9 (suggesting that despite intense support for Digital ID among international organizations like UNICEF and the World Bank, such programs often cause more harm than good); *see also, e.g.*, Chip Johnson, *How Oakland fouled up ID card plan*, SFGate (Mar. 21, 2013), https://www.sfgate.com/bayarea/johnson/article/how-oakland-fouled-up-id-card-plan-4374916.php [https://perma.cc/JNZ5-UY2A] (reporting how San Francisco built a Digital ID system in partnership with a corporate vendor that charged exorbitant fees for the ID's debit card feature).

credential used to provide or restrict access to government resources. The site offers remote authentication and verification services so that agencies can establish individual users' uniqueness and match them to a real-world identity. As of May 2024, over one hundred million individuals had created Login.gov user accounts in order to access over 480 government websites and services.[6] And the credential could eventually be used as an alternative to Apple ID or Google accounts in the private sector, too.[7] The platform centralizes a process previously dispersed across agencies, and digitizes one previously handled by people and paperwork. Early-stage design choices have impacted and will continue to determine long-term realities of what the government offers, to whom, and on what terms.

The stakes are high. Login.gov is a major infrastructural undertaking that affects how the government relates to its constituents. If it doesn't work, people will lose access to needed government resources.[8] Law enforcement will inevitably demand access to whatever information Login.gov collects and stores about people.[9] This matters not only because increased police power disproportionately endangers marginalized communities, but also because those communities may shy away from claiming needed government benefits out of fear of such surveillance. As the platform's user base and implementations expand, so does the risk of a catastrophic data breach.[10] In short, the public has an interest in a reliable, safe, non-punitive, and equitable platform for

[6] Login.gov: Program Roadmap 7 (May 2024), https://www.login.gov/docs/login-gov-roadmap-may-2024.pdf [https://perma.cc/PXG7-VNBH].

[7] *See* Axel Domeyer, Mike McCarthy, Simon Pfeiffer & Gundbert Scherf, *How Governments Can Deliver on the Promise of Digital ID*, McKinsey & Co. (Aug. 31, 2020), https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id [https://perma.cc/EK2H-AXFM] ("Digital ID supports consumers and businesses through benefits that include streamlined registration and authentication processes, secure digital payments, and digital high-assurance contracting."); *cf. Government Records & Privacy*, Elec. Priv. Info. Ctr., https://epic.org/issues/data-protection/government-records-privacy [https://perma.cc/2TJ8-EAER] (discussing how social security numbers were initially only for government use but their usefulness as a unique identifier led them to become common in private sector usage too).

[8] *Cf.* Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, Verge (Mar. 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/Z6BE-3F2J] (describing how a faulty algorithm arbitrarily denied health care to people in Arkansas).

[9] Data-maximizing infrastructures have a way of enhancing police power in unexpected ways. Consider cellphone towers: When they first went up, nobody anticipated that the location data they generate would lead to a new era of Fourth Amendment jurisprudence. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214–15 (2018) (describing how Fourth Amendment jurisprudence has evolved with technological innovation).

[10] *See, e.g.*, Sean Gallagher, *Baltimore Ransomware Nightmare Could Last Weeks More, With Big Consequences*, Ars Technica (May 20, 2019), https://arstechnica.com/information-technology/2019/05/baltimore-ransomware-nightmare-could-last-weeks-more-with-big-

accessing government resources online.[11] No one legal framework is sufficient to protect this interest: Privacy and Due Process rights can be vindicated only through grueling case-by-case litigation; antitrust and consumer protection laws don't apply against the government. Infrastructural design matters because "[i]t shapes juridical relations and imaginaries."[12] If Login.gov fails to serve the public interest, it risks permanently eroding the public's wellbeing, rights, and overall trust in government.

In this Note, I critically examine how the federal government went about designing and building Login.gov, and the social, technical, and legal consequences of those choices. I argue that the General Services Administration (GSA)—the government body in charge of government operations, including Login.gov—made critical missteps due to a "move fast and break things" mentality ill-befitting a government agency, leading them to disregard critical infrastructural values.[13] In particular, I critique the GSA's decision to make Login.gov's core functions dependent on tools designed and operated by LexisNexis, a data broker with a notoriously extractive and non-transparent business model.[14] I argue that when designing digital infrastructure, the government must behave like a government, not a startup. Instead of expediency,

consequences [https://perma.cc/TNB5-TMFV] (reporting how a ransomware attack on the City of Baltimore's networks caused weeks of chaos in the city).

[11] In focusing on Login.gov as an infrastructure, I take inspiration from Professor Benedict Kingsbury's work on infrastructure as regulation (or "InfraReg"). *See* Benedict Kingsbury, *Infrastructure and InfraReg: On Rousing the International Law 'Wizards of Is*,' 8 Cambridge Int'l L.J. 171, 179 (2019) ("Thinking infrastructurally typically entails understanding infrastructure not simply as a thing, but as a set of relations, processes and imaginations. One well-established approach brings together in infrastructural thinking the technical . . . the social . . . and the organisational . . . . It is only possible to understand the processes of infrastructure, and the consequences or potential of any intervention in infrastructure, by fully exploring each of these and their joint interactions and effects.").

[12] *Id.* at 182.

[13] The reference to "move fast and break things" refers to a phrase coined by Mark Zuckerberg to describe the startup attitude of acting without fear of making mistakes, and dealing with the fallout after the fact. *See Mark Zuckerberg's Letter to Investors:* 'The Hacker Way,' Wired (Feb. 1, 2012), https://www.wired.com/2012/02/zuck-letter [https://perma.cc/AF2H-PJ3D].

[14] LexisNexis verifies most Login.gov user accounts against its own database of over 84 billion records scraped from across the internet, as discussed at length in Section I.B.2. *See* LexisNexis Risk Solutions (LNRS) Identity Proofing: Privacy Impact Assessment, Gen. Servs. Admin. 12 (Sept. 15, 2022), https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems [https://perma.cc/BHB2-EN9R] [hereinafter LexisNexis PIA]; *Search Public Records*, LexisNexis, https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page [https://perma.cc/QN4H-YH4Y]. Readers will know LexisNexis for its useful legal research tools, and perhaps for its controversial $22.1 million data sharing contract with Immigration and Customs Enforcement. *See* End the Contract Coalition, https://endthecontract.wixsite.com/home [https://perma.cc/DVZ2-BQDC].

infrastructural projects in the digital age must prioritize transparency, equity, and participatory design. I posit that this imperative is reflected in the Privacy Act of 1974's famous Fair Information Practice Principles, if not in the Act's current regulatory structure.

This Note proceeds as follows. In Part I, I explain how Login.gov actually works, including the critical role LexisNexis plays in its operations. I describe the technical processes the site uses to ensure that each account is used by only one user ("authentication") and that each user is in fact the real-world person she claims to be ("verification"). This technical section is critical for understanding the GSA's design decisions when building Login.gov, and for appreciating those decisions' infrastructural significance. I highlight how, by partnering with LexisNexis for user verification, Login.gov entrenched LexisNexis's corporate interest in data extraction, exclusion, and technical obscurity within a government system that should advance privacy, access, and transparency.

In Part II, I describe how the Login.gov-LexisNexis partnership developed and the trouble it caused for the GSA. I argue that the GSA's search for expedient solutions impeded Login.gov's ability to serve the public's interest in secure, equitable, efficient, and privacy-protective digital infrastructure. I tell how, in 2023, a watchdog agency accused Login.gov of intentionally misleading and defrauding its government customers about the platform's verification capabilities. I discuss how this scandal resulted from the GSA's rush to roll out Login.gov, leading it to partner with LexisNexis before seeking community input or gaining the public's trust in the project.

Finally, in Part III, I discuss solutions for Login.gov and digital infrastructure going forward. I suggest that the post-Nixon administration Congress that passed the Privacy Act of 1974 understood the importance of trustworthy digital infrastructure, even if they could not conceptualize the particular risks and benefits of a Digital ID system like Login.gov. I contend that the Privacy Act's Fair Information Practice Principles reflect an admirable grappling with the significance of infrastructural design in the digital age, and that truly trustworthy digital infrastructure will treat these principles as foundational commitments.

I
Login.gov: America's National Digital ID

Identities are multifaceted, but not every facet of an individual's identity is relevant in every scenario. One person may identify as a nurse, an immigrant, a brother, and a guitar player, but when joining a local running group, all he needs to share is that he lives in Brooklyn and runs an eight-minute mile. He proves that these assertions are trustworthy by showing up for, and keeping up with, the running group.

When it comes to accessing government services—including schools, courts, and welfare benefits—the stakes are higher, and the government needs a way to establish the uniqueness of individuals. The relevant aspect of an individual's identity in such cases is often their legal identity.

Legal identity gives a person recognition before the law. It is not the same thing as citizenship or any other legal status; it is a far more basic level of recognition that establishes the uniqueness of a person's name, sex, date of birth, and place of birth. The United Nations Statistics Division defines legal identity as "the basic characteristics of an individual . . . conferred through registration and the issuance of a certificate by an authorized civil registration authority."[15] Legal identity enables participation in civil society through voting, banking, owning and renting property, marriage, education, and more.[16] Lack of legal identity therefore leads to political non-recognition, social marginalization, and exclusion from economic benefits.[17] The right to a legal identity is enshrined in the Universal Declaration of Human Rights, signifying its fundamental importance in modern life.[18] Assertions of legal identity are rendered trustworthy through credentials typically issued by government authorities like passports, Social Security Numbers, or driver's licenses.

Unlike many other countries, the United States does not require its residents, citizens, or constituents to carry a physical national identity card that confirms legal identity.[19] A nationwide identity credential does not even exist in the United States. Past attempts to create a national ID system have been met with adamant opposition. When some states

[15] *United Nations Legal Identity Agenda*, U.N. Stat. Div., https://unstats.un.org/legal-identity-agenda [https://perma.cc/7ZEE-4MQ5]; *see also* Dashiell Allen & Roberto Bolaños, *IDNYC Card: What It Is, How to Apply and Its Benefits*, Documented, https://documentedny.com/2021/02/26/idnyc-card-what-is-how-to-apply-and-its-benefits [https://perma.cc/2JQG-DUZC] (demonstrating how undocumented immigrants can access fundamental services through use of this ID card that does not depend on legal residency).

[16] *See* U.S. Agency for Int'l Dev., Identity in a Digital Age: Infrastructure for Inclusive Development 4 (2022), https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf [https://perma.cc/UB8A-8KVG].

[17] *See generally id.* at 1.

[18] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 8, 1948), Art. 6 ("Everyone has the right to recognition everywhere as a person before the law.").

[19] Nathaniel Kim, *National ID for Public Purpose*, 7 Geo. L. Tech. Rev. 272, 275 (2023) ("[T]he United States finds itself in the minority when it comes to the adoption of a national ID system—out of nearly 200 countries in the world, at least 170 have established some form of national ID or plan to implement one.").

introduced a proposal to standardize driver's licenses nationwide after 9/11, a coalition of groups from across the political spectrum wrote a letter to the Bush Administration urging against this "bureaucratic back door" effort to create a national ID.[20] Civil rights advocates emphasize that national ID systems can be used to exclude people from rights and benefits, swell police control, and discriminate against marginalized groups.[21] Conservatives criticize national ID systems as unnecessary expansions of government power.[22] As one voting rights advocate told The Atlantic: "There are only three problems with a national ID: Republicans hate it, Libertarians hate it, and Democrats hate it . . . ."[23]

Instead of a national ID card, Americans—including citizens, green card holders, and other residents—can prove their legal identity with any number of government-issued credentials, each with its own distinct purpose. Passports prove legal identity as well as national citizenship, though fewer than half of Americans have a valid passport.[24] Driver's licenses prove legal identity as well as state residency and, in some states, immigration status, but not national citizenship.[25] Social security numbers prove legal identity as well as legal residency, and most Americans have one, but they are notoriously easy to steal because

[20] *See* Letter from the American Civil Liberties Union to George W. Bush, President of the United States (Feb. 11, 2002) (on file with author), https://www.aclu.org/legal-document/coalition-letter-president-bush-urging-him-reject-national-id-card?redirect=technology-and-liberty/coalition-letter-president-bush-urging-him-reject-national-id-card [https://perma.cc/MM3E-TSWV] (including sign-on from groups such as the Libertarian Party and the Multiracial Activist and Abolitionist Examiner, among others).

[21] *See, e.g.*, *Mandatory National IDs and Biometric Databases*, Elec. Frontier Found., https://www.eff.org/issues/national-ids [https://perma.cc/C6KR-Y58A] (explaining that national ID systems "increase the power of authorities to reduce your freedoms to those granted by the card," thus facilitating abusive police behavior and discriminatory state conduct).

[22] *See, e.g.*, Jim Harper, CATO Inst., The New National ID Systems 3–5 (Jan. 30, 2018), https://www.cato.org/sites/cato.org/files/pubs/pdf/pa-831-updated.pdf [https://perma.cc/YSE2-6CBU] (discussing how the United States' new national ID systems present a threat to liberty and privacy).

[23] Russell Berman, *The Obvious Voting-Rights Solution That No Democrat Will Propose*, Atlantic (Aug. 30, 2021), https://www.theatlantic.com/politics/archive/2021/08/voting-rights-national-id-card/619772 [https://perma.cc/WL2Y-N9YT].

[24] *Reports and Statistics: U.S. Passports*, U.S. Dep't of State Bureau of Consular Affs., https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html [https://perma.cc/XM5Q-TGXB] (reporting the number of valid passports in circulation in 2023 as 160,668,889, which is about 48% of the U.S. population).

[25] In New York, lawful status is not required to obtain a driver license. *See Get Your Learner Permit and First Driver License*, Dep't of Motor Vehicles, https://dmv.ny.gov/driver-license/get-your-learner-permit-and-first-driver-license [https://perma.cc/X94A-NZCA]. By contrast, in Missouri, a resident cannot obtain a driver license without proving lawful residency. *See Documents for Driver License, Nondriver ID, and Instruction Permit*, Mo. Dep't of Revenue, https://dor.mo.gov/driver-license/issuance/id-requirements.html [https://perma.cc/922F-HUJB].

there is no way to verify that the number actually belongs to the person presenting it.[26]

There is no single national credential that reliably ties a person's legal identity to all these other pieces of information. But it is possible to connect the dots between these disparate public records. This is what the data broker industry does. Data brokers like LexisNexis collect records from around the internet, including public records scraped or purchased directly from the government, and compile them into a comprehensive picture that can easily identify someone online. These "middlemen of surveillance capitalism" sell access to the aggregated data to law enforcement, advertising agencies, and anyone else willing to pay.[27] In making the case for a national ID system, a recent law review article referred to the data broker industry as a de facto national ID system, but one built upon perverse incentives "to extract from the people, rather than to serve them."[28] Yet, instead of constructing an alternative with democratically selected priorities and trust-enhancing safeguards in place, the GSA decided to build Login.gov to depend on precisely this business model.

A. What Is Digital ID?

In contrast to physical identity credentials that can be carried in a pocket and handed over to a TSA agent or landlord, digital identity refers to a credential used to identify a real-world person remotely, in the digital sphere. As core civil society functions and government services move online, it is increasingly critical to develop digital infrastructure that can reliably link an internet user to her real-world legal identity. These "Digital IDs" must *authenticate* that the internet user is a real person and *verify* that the person is in fact who she claims to be. This is the project of Login.gov.

Digital ID has the capacity to vastly increase access to government resources, but it can also create new means of excluding and marginalizing underserved populations. Many in the international development community have lauded Digital ID as an "accelerator of inclusion," and

[26] *See* Suzanne Rowan Kelleher, *Everyone's Social Security Number Has Been Compromised. Here's How to Protect Yourself*, Forbes (Aug. 1, 2019), https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=6ea189929ac7 [https://perma.cc/K6N8-LT9P] (explaining the vulnerability of SSNs given they have no verification method associated with them).

[27] *See* Kim, *supra* note 19, at 289.

[28] *Id.*

countries around the world have invested in Digital ID infrastructure.[29] The Obama Administration made developing secure, publicly-operated digital access to government resources a key priority.[30] But when a Digital ID system is difficult to use, the results can be disastrous. This is especially true for populations without access to technology or historically vulnerable groups with good reason to fear government data collection.[31] In political systems plagued by discriminatory bias, Digital IDs can make it easier for governments to discriminate.[32] And automated fraud prevention mechanisms can disproportionately exclude groups whose profiles do not match the training data, such as unbanked people, new immigrants, or people with disabilities.[33]

Realizing the increasingly critical role Digital ID is set to play in governance, U.S. government agencies and authorities began developing

[29] *See* Katelyn Cioffi, Victoria Adelmant, Danilo Ćurčić, Brian Kiira, Grecia Macías & Yasah Musa, *Contesting the Foundations of Digital Public Infrastructure: What Digital ID Litigation Can Tell Us About the Future of Digital Government and Society*, Ctr. for Human Rts. and Glob. Just. at N.Y. Univ. L. 3 (Aug. 28, 2023), https://drive.google.com/file/d/13o8DBZsOArYOpsxvt3z689T0xPtiQdX8/view [https://perma.cc/LKQ4-RR6Q]; *see also generally* Mariana Rozo-Paz, Jack Smye, & Sourav Panda, *Enhancing Inclusion in Digital Identity Policies and Systems*, Berkman Klein Ctr. for Internet & Soc'y at Harv. Univ. (2023), https://drive.google.com/file/d/1VxiwB22sEpidzd1kgZt93aIIcOflVFvU/view [https://perma.cc/9SRP-G6FD] (articulating an inclusive framework for implementation of digital identity).

[30] *See* Fact Sheet, *Cybersecurity National Action Plan*, White House (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [https://perma.cc/9JFY-QMMP] (announcing the Administration's plan to enhance cybersecurity infrastructure).

[31] *See, e.g.*, Katelyn Cioffi, *Human Rights Gateway or Gatekeeper: Digital IDs on Trial in Uganda*, Open Global Rights (July 24, 2023), https://www.openglobalrights.org/human-rights-gateway-gatekeeper-digital-ids-uganda [https://perma.cc/4UT9-JYGX] (reporting how Uganda's faulty national ID rollout led to mass exclusion of marginalized groups); Ctr. on Hum. Rts. and Glob. Just. at N.Y. Univ. L., Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons 9–14 (2021) (same).

[32] *See, e.g.*, Nanjala Nyabola, *National Digital ID Initiatives Have a Trust Problem*, Rest of World (May 5, 2021), https://restofworld.org/2021/kenya-digital-id [https://perma.cc/ZDQ3-S8ML] (describing how preexisting discrimination, power disparities, and exclusionary systems were embedded in Kenya's kitambulisho Digital ID, wasting needed resources on a system designed without community input that was advertised as distributing benefits but in fact served to increase state control and police power).

[33] *See generally* Elizabeth Bynum Sorrell & Ariel Kennan, *Digital Authentication and Identity Proofing in Public Benefits Applications*, Digit. Benefits Network at the Beeck Ctr. for Social Impact + Innovation at Geo. Univ. (May 19, 2023), https://www.digitalbenefitshub.org/publications/digital-authentication-and-identity-proofing-data [https://perma.cc/QP6N-WBZE] (discussing how certain methods of identity proofing can disproportionately impact vulernable groups); ACLU and Elec. Priv. Info. Ctr., Comment on NIST's 2023 Digital Identity Guidelines 12–13 (Apr. 14, 2023) ("Internet users with disabilities may also be disproportionately flagged by poorly designed fraud monitoring tools because their behavioral patterns will differ from abled users.").

digital identity platforms. Some built their own tech, some used private sector tools, some a combination. But this system of patchwork digital identity tools was inefficient, expensive, and unreliable.[34] So in April 2017, the federal government launched Login.gov, a nationwide Digital ID designed with the goal of "increas[ing] equitable access to benefits and services while reducing fraud and protecting taxpayer dollars."[35]

B. *What Is Login.gov? How Does It Work?*

Login.gov is a secure login service built and managed by the General Services Administration (GSA).[36] The GSA is a federal agency that supports the operations of the federal government through acquiring and managing office space, technology services, and other products on behalf of other agencies.[37] Believing that the existing system of disparate applications across government sites created "an inconsistent, confusing, or unreliable user experience," the GSA designed Login.gov to provide a "seamless user experience [that] directly improves the customer's quality of life, engenders faith in government services, and improves security and privacy protections."[38]

Login.gov is designed to work as a single-sign-on platform for any government agency—federal, state, or local—that chooses to use it.[39] Individuals can access all partnering agencies' services using just one username and password instead of going through a different log-in process with each agency. Meanwhile, partnering agencies get to outsource their user authentication and verification processes to Login.gov, a trusted government partner.[40] As of September 2023, over forty

[34] *See* Joel Minton & Tom Mills, *Government Launches Login.gov to Simplify Access to Public Services*, 18F (Aug. 22, 2017), https://18f.gsa.gov/2017/08/22/government-launches-login-gov [https://perma.cc/6693-T28T].

[35] *Login.gov Continues to Expand, Offering New Pathways to Securely Accessing Government Services Online*, U.S. Gen. Servs. Admin. (Oct. 18, 2023), https://www.gsa.gov/blog/2023/10/18/logingov-continues-to-expand-offering-new-pathways-to-securely-accessing-government-services-online [https://perma.cc/N5YP-XHTV]; *see also* Minton & Mills, *supra* note 34 (announcing the April 2017 launch of Login.gov and stating that it is designed to "improve[] the customer's quality of life, engender[] faith in government services, and improve[] security and privacy protections").

[36] Login.gov, *supra* note 1.

[37] *See Our Mission's Evolution*, U.S. Gen. Servs. Admin. (Mar. 20, 2024), https://www.gsa.gov/about-us/mission-and-background/our-missions-evolution?topnav=about-us [https://perma.cc/87YM-KKYT].

[38] Minton & Mills, *supra* note 34.

[39] *State, Local, and Territories*, Login.gov Partners, https://www.login.gov/partners/state-and-local [https://perma.cc/NJ69-PKMB].

[40] *See What is the Benefit of Partnering with Login.gov?*, Login.gov Partners, Frequently Asked Questions, https://www.login.gov/partners/faq [https://perma.cc/FB86-UPZZ]; *see also U.S. General Services Administration Announces All Cabinet Agencies Are Now Using Login.gov*, U.S. Gen. Servs. Admin. (Sept. 29, 2023), https://www.gsa.gov/about-us/newsroom/

federal and state agencies partnered with Login.gov for at least one program or application.[41] Over one hundred million individual users have created a Login.gov profile.[42]

Login.gov provides two services: authentication and verification. When a user creates an account, the site will first *authenticate* that she is the only person who can access that account. Next, it will *verify* that the information the user submits about her legal identity really belongs to her. There are many ways to accomplish authentication and verification, each bearing particular benefits and risks. Key questions of efficiency, equity, privacy, and security are buried in the technical details. Thus, in order to understand the social and legal significance of the GSA's business and design choices in developing Login.gov, it is critical to first understand how the platform's technology actually works.

1. Authentication

Authentication is the process by which Login.gov ensures that a user accessing the account is the same person who created it, not an imposter. When an individual user creates a Login.gov account, she is required to provide an e-mail address, a password, and one or more additional authentication methods.[43] This is called two-factor authentication ("2FA"), meaning that every time a user attempts to log in using her Login.gov username and password, she will have to prove that she is actually herself by interacting with a secondary authentication mechanism.[44]

2FA works by linking two security factors associated with the same individual. Security experts refer to three categories of security factors: (1) "something you know," like a username or password; (2) "something you have," like a mobile device or a thumb drive; and (3) "something you are," like a thumbprint or face scan.[45] By requiring 2FA, Login.gov

news-releases/us-general-services-administration-announces-all-cabinet-agencies-are-now-using-logingov-09292023 [https://perma.cc/Y7AA-JR6B] ("Login.gov is continuing to expand its capabilities further to provide the public with a simple, secure, equitable, and privacy-protecting solution to access government services.").

[41] *U.S. General Services Administration Announces All Cabinet Agencies Are Now Using Login.gov*, *supra* note 40.

[42] Login.gov: Program Roadmap, *supra* note 6, at 7.

[43] *Create an Account*, Login.gov, https://login.gov/create-an-account [https://perma.cc/GM9C-6DGW].

[44] *Glossary*, NIST Compt. Sec. Res. Ctr., https://csrc.nist.gov/glossary/term/2fa [https://perma.cc/A3H8-TYBR].

[45] *See Two-Factor Authentication Explained: How to Choose the Right Level of Security for Every Account*, PCWorld (Apr. 10, 2019), https://www.pcworld.com/article/403535/two-factor-authentication-faq-sms-authenticator-security-key-icloud.html [https://perma.cc/DA4H-KGE3].

requires every user to not only prove knowledge of her username and password, but also to prove one of these other security factors.[46]

Internally, Login.gov also assigns each authenticated account a master Universally Unique Identifier (UUID), which identifies the user within Login.gov.[47] A UUID is a 128-bit piece of encoded data, generated using an algorithm that ensures its uniqueness.[48] A user's master UUID is used only within Login.gov, but Login.gov also generates an additional, agency-specific UUID associated with each agency that the user accesses via Login.gov.[49] When a user accesses a new partner agency site for the first time, Login.gov obtains consent from the user to share each piece of information about the user that the partner agency requires for its registration process.[50] The partner agencies can use the agency-specific UUID to store information about the user—either information that the user shared upon registration, or information about the user's interactions with the application. The agencies do not have access to information associated with the user's master UUID or other agency-specific UUIDs.[51]

A Login.gov user who has created a username and password, set up at least one secondary authentication method, and been assigned a master UUID is identifiable as unique within the Login.gov system. She has been "authenticated."

[46] Login.gov requires users to set up one secondary authentication method, and encourages users to set up multiple methods. Login.gov accepts a wide variety of secondary authentication methods that will be familiar to many readers, including authentication applications like LastPass or Authy, codes sent by text message or phone call, security keys, and backup codes. These methods all aim to confirm that the person accessing the Login.gov account has access to a specific physical item—cell phone, thumb drive, or list of backup codes—that she also possessed at the time of account creation. A biometric comparison can also be used for authentication, as it confirms "something you know" with "something you are." *See id.*; *see also Authentication Methods*, LOGIN.GOV, https://login.gov/help/get-started/authentication-methods [https://perma.cc/6GST-KPS8].

[47] RICHARD SPEIDEL, LOGIN.GOV PRIVACY IMPACT ASSESSMENT, GENERAL SERVICES ADMINISTRATION 7 (May 14, 2024), https://www.gsa.gov/system/files/Login.gov_PIA_%28May_2024%29.docx.pdf [https://perma.cc/5ER2-YSMA] [hereinafter LOGIN.GOV PIA].

[48] *See* P. Leach, M. Mealling & R. Salz, *Request for Comments: 4122, A Universally Unique IDentifier (UUID) URN Namespace*, NETWORK WORKING GROUP (July 2005), https://www.rfc-editor.org/rfc/rfc4122 [https://perma.cc/X74Y-W3G5] (describing five algorithms that can be used to generate UUIDs, which ensure that the probability of a duplicate UUID is close to zero).

[49] *See* LOGIN.GOV PIA, *supra* note 47, at 8–9 nn.11–12 ("Login.gov does not share the Master UUID with third-party providers for the purpose of authentication or identity verification . . . .").

[50] *See id.* at 14 ("Login.gov does not make data actions (e.g., sharing a user's information with a partner agency) without the user's consent.").

[51] *Id.* at 15.

2. *Verification*

Authentication is the first step, but verification is what tethers the user to a real-world legal identity. In other words, any information Login.gov has about the user before verification is "self-asserted," not externally confirmed.[52] For some partner applications this is a sufficient level of assurance. Users will be able to access those applications without providing any further information to Login.gov.

However, other partner applications require users to verify their real-life legal identity. For example, in order to offer an online tax-filing service, the IRS needs to limit log-ins to users who have proven that they are who they claim to be.[53] And as the need for Americans to access benefits online spiked during the COVID-19 pandemic, there was an accompanying spike in identity theft, with government documents or benefits fraud as the largest category of resulting frauds.[54] Login.gov advertises verification through a process it calls "identity proofing," which requires a user to provide a state-issued ID (driver's license or state-issued non-driver's ID card), a Social Security number, and a phone number associated with a mailing address (or just the mailing address).[55] Once a user has verified her identity to Login.gov, she will be able to access all partner applications without any further verification.

There are a variety of ways to do identity proofing. Some methods involve knowledge-based verification, where the applicant answers questions about her credit history.[56] Some involve biometric comparisons such as faceprint or fingerprint matching.[57] In 2024, Login.gov announced plans to offer several new verification options,

[52] The National Institute of Standards and Technology refers to this as "Identity Assurance Level 1" (IAL1). Paul A. Grassi & James L. Fenton, Special Publication 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing, NIST § 2.2 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf [https://perma.cc/SP6M-W5JX] [hereinafter Digital Identity Guidelines: Enrollment and Identity Proofing].

[53] *See* Treasury Inspector General for Tax Administration, Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification 9 (Sept. 27, 2023).

[54] Fed. Trade Comm'n, Consumer Sentinel Network Data Book 15 (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf [https://perma.cc/4L9K-567A].

[55] *How to Verify Your Identity*, Login.gov, https://login.gov/help/verify-your-identity/how-to-verify-your-identity [https://perma.cc/HL4N-VTDN].

[56] *See, e.g.*, *Questions and Answers about Remote Identity Proofing and Multi-Factor Authentication*, Centers for Medicare and Medicaid Services 1 (Oct. 2015), https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Downloads/HETSHPGRIDPMFAFAQ.pdf [https://perma.cc/UJJ9-WQRP].

[57] *See, e.g.*, Paresh Dave, *States using ID.me, Rival Identity Check Tools for Jobless Claims*, Reuters (July 22, 2021), https://www.reuters.com/business/states-using-idme-rival-identity-check-tools-jobless-claims-2021-07-22 [https://perma.cc/VR8F-B7L5] (comparing selfies to official photo documentation).

including in-person verification at U.S. Post Offices, remote verification via video conference, and a facial recognition option.[58] But for at least its first six years of existence, Login.gov offered only one verification option: third-party identity proofing conducted by LexisNexis.[59] And LexisNexis verification remains the default.[60]

In order to verify a user's identity, Login.gov relays information about the user to LexisNexis.[61] LexisNexis utilizes a variety of "solutions" to verify a user's identity based on the information she conveys to Login.gov.[62] LexisNexis attempts to verify a wide variety of real-world identifiers, including but not limited to:

- Date of birth
- Deceased
- Occupancy
- High-risk address
- Phone checks (phone type, status, CallerID)
- Signs of "high-risk digital behavior"
- Biometric and behavioral data such as how a user touches and moves her device while using Login.gov
- Whether the information visible on the ID submitted matches the information encoded in the ID's barcode and magstripe
- Email address metadata, including "domain details, email details, risk indicators, and when available, other personally identifiable information"
- "Hundreds of unique identity characteristics and life events" gleaned from consumer, asset, and business records[63]

LexisNexis's most important verification tool is a patented technology called Scalable Automated Linking Technology ("SALT"). SALT is an algorithm that handles data integration tasks, including

[58] *Login.gov Continues to Expand, Offering New Pathways to Securely Accessing Government Services Online*, GSA Blog (Oct. 18, 2023), https://www.gsa.gov/blog/2023/10/18/logingov-continues-to-expand-offering-new-pathways-to-securely-accessing-government-services-online [https://perma.cc/DD2J-Q7WT].

[59] *See id.* ("[New verification methods] build on top of Login.gov's existing identity verification process, which requires validation of a government-issued ID and a phone number or address.").

[60] *See* Privacy Impact Assessment (May 14, 2024), Login.gov 20–21, https://www.gsa.gov/system/files/Login.gov_PIA_%28May_2024%29.docx.pdf [https://perma.cc/5SRR-Y6WG].

[61] *See* LexisNexis PIA, *supra* note 14, at 6 (explaining that LexisNexis is the identity proofing program for Login.gov).

[62] *See id.*

[63] *Id.* at 6–7.

"record linkage."[64] Record linkage is the process by which records from disparate data sources are determined to refer to the same real-world entity.[65]

At a very high level, record linkage works by training an algorithm to recognize how closely the data in one field of Dataset A (for example, "name") corresponds with the data in the fields of Dataset B (for example, "full name" or "age").[66] This allows the algorithm to determine which fields in each dataset are more likely to contain matching information when records from these respective datasets refer to the same person. LexisNexis aggregates data from tens of thousands of internet sources in this way.[67] So, when a record from Dataset A is compared with a record from Dataset B, the algorithm can calculate the probability that the records refer to the same person based on whether the data matches in the expected fields. Fields that are more likely to contain matching information are weighted more heavily in this calculation (for example, "name" and "full name"), whereas fields that are less likely to contain matching information are weighted less heavily (for example, "first name" and "last name").[68] As the SALT algorithm learns more about a dataset, it learns to weight data within fields more heavily for rare values (such as "Zakarchuk" or "Yuma") and less heavily for common values (such as "Smith" or "Johnson").[69]

Once a set of records has been "internally linked" through this process, SALT can also be used to perform "external linking." Also known as "entity resolution," this process algorithmically matches data from an external file or query to an identity in the internally-linked database.[70] In order to do this, the SALT user can identify which fields in an external record correspond with fields in the internally-linked

[64] *See generally* Anthony M. Middleton & David Alan Bayliss, *Salt: Scalabale Automated Linking Technology for Data-Intensive Computing*, *in* HANDBOOK OF DATA INTENSIVE COMPUTING 189–234 (Borko Furht & Armando Escalante eds., 2011) (presenting two LexisNexis employees' explanation of how LexisNexis's record linkage technology works).

[65] *Id.* at 191.

[66] *Id.*

[67] By its own count, LNRS's database includes over 84 billion records from over 10,000 sources. *See Search Public Records*, LEXISNEXIS, https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page [https://perma.cc/QN4H-YH4Y].

[68] *See* Middleton & Bayliss, *supra* note 64, at 191.

[69] *See id.* at 201–02. According to the 2010 U.S. Census, "Smith" and "Johnson" were the first and second most common last names, and "Zakarchuk" and "Yuma" were two of the least common last names with 100 or more occurrences. *See Frequently Occurring Surnames from the 2010 Census*, U.S. CENSUS BUREAU, https://www.census.gov/topics/population/genealogy/data/2010_surnames.html [https://perma.cc/9AF4-FPMG] [hereinafter *Frequently Occurring Surnames from the 2010 Census*].

[70] Middleton & Bayliss, *supra* note 64, at 225.

database, and can designate which fields *must* match in order for the external record to link with an entity in the internally-linked database.[71]

SALT record linkage is not a fool-proof system. It inherently bears the risk of both false positives (when a fraudster gets through) and false negatives (when a genuine applicant is wrongly denied access).[72] SALT users set a probability threshold above which two records are deemed a match, meaning that they refer to the same real-world person, and below which the two records are considered a non-match.[73] As a security tool designed to prevent fraud, LexisNexis is primarily concerned with excluding false positives. But this is troubling in the context of Login.gov, an infrastructure ostensibly intended to help people access needed government resources more efficiently.[74] Moreover, the accuracy of a given match improves as more records are compiled about a person.[75] LexisNexis record linkage results are less nuanced, and likely less accurate, as to people without many records in the public databases that the SALT algorithm scrapes. This means that people without credit or without a long history in the U.S. are likely more often denied access to Login.gov.

Login.gov's Help Center does not provide guidance on what a user should do if their identity verification process fails.[76] The GSA's Privacy Impact Assessment of Login.gov's partnership with LexisNexis ("LexisNexis PIA") provides that a user must contact LexisNexis directly to view or amend the information that LexisNexis has in their profile.[77] The LexisNexis PIA directs people who wish to correct the records LexisNexis maintains about them to a "Description of Procedure Letter," which promises nothing except that "[i]f the consumer provides source-based evidence proving their position, LexisNexis will include this information in its reinvestigation procedure."[78]

[71] *Id.* at 225–27.

[72] *Id.* at 224 ("It is not uncommon to have some false positives and false negatives in a linking process.").

[73] *Id.* at 222. SALT can also set a default, algorithmically-calculated threshold. *Id.*

[74] Louise Amoore refers to this style of identification as "governing by identity," and writes that this security-oriented form of governance contributes to "a lack of social space in which we can see and be seen, engage with the differences and difficulties of our world." *See* Louise Amoore, *Governing by Identity*, *in* Playing the Identity Card: Surveillance, Security and Identification in Global Perspective 21–36 (Colin J. Bennett & David Lyon eds., 2013).

[75] *See* Middleton & Bayliss, *supra* note 64, at 222.

[76] *See How to Verify Your Identity*, *supra* note 55.

[77] *See* LexisNexis PIA, *supra* note 14, at 19; *see also Description of Procedure*, LexisNexis Consumer Center, https://consumer.risk.lexisnexis.com/img/Dispute_Process_Steps.pdf [https://perma.cc/96ZK-UKYS].

[78] *Description of Procedure*, *supra* note 77.

3. *A Brief Word on Authorization*

Login.gov provides authentication services and verification services as described above, but Login.gov does not control authorization. In other words, each partner application decides for itself what information about a user it requires before that user is permitted to access its services, and each user decides what information about herself she wants to share with partner applications. These pieces of information are called "user attributes."[79]

The National Institute of Standards and Technology established a system of Identity Assurance Levels ("IALs") for digital identity tools, which is an example of an authorization framework. According to the guidelines, which I discuss further in Section II.B, any agency using digital identity tools is required to assess its own security risks and "the potential harm caused by an attacker making a successful false claim of an identity."[80]

Based on that assessment, the agency determines which of three IALs it must achieve. "IAL1," the lowest level, does not require any link between the digital identity applicant and a real-world identity, so user access may be authorized based solely on self-asserted, non-verified information.[81] "IAL2" requires evidence that "supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity."[82] Without verified evidence, the user will not be authorized to access the government resources. "IAL3" requires in-person identity proofing by a trained representative of the digital identity provider before user access is authorized.[83] The IAL system recognizes that different Digital ID implementations bear different risks and, at least in theory, enables agencies with fewer security concerns to implement Digital ID with a lower barrier to entry.

When a Login.gov user attempts to access a partner application for the first time, the partner application—having determined which IAL applies to them—requests its required user attributes from Login.gov. If Login.gov has successfully *verified* those user attributes, it will confirm with the user that she wants to share the information with that application, and will then share the verified user attributes

[79] *See User Attributes*, LOGIN.GOV, https://developers.login.gov/attributes [https://perma.cc/UKH3-J9UL].

[80] PAUL A. GRASSI, MICHAEL E. GARCIA & JAMES L. FENTON, SPECIAL PUBLICATION 800-63-3: DIGITAL IDENTITY GUIDELINES, NIST vi (June 2017), https://doi.org/10.6028/NIST.SP.800-63-3 [https://perma.cc/2CTQ-JJBD] [hereinafter DIGITAL IDENTITY GUIDELINES].

[81] *Id.*

[82] *Id.*

[83] *Id.*

with the requesting application. The user is then *authorized* to use the application, and the application is authorized to access the user's information. Each time that user attempts to access that partner application, the application will ask Login.gov to *authenticate* that the login attempt is coming from the user herself.

II
The Login.gov-LexisNexis Partnership: How It Happened & Why It Matters

When the GSA first began developing Login.gov in 2016, its team of technologists announced the agency's hope that Login.gov would "improve the public's online safety and security," while simultaneously "creating a user experience that is painless and intuitive, thus lowering any barriers to entry for people who depend on access to their online information without compromising security."[84] This Part discusses how important values such as security, equity, efficiency, and privacy all motivated the development of Login.gov, but not always equally, and not all at the same time. Unfortunately, the GSA's rush to launch Login.gov led them to an ill-considered partnership with LexisNexis that compromised each of these goals.

In an infrastructure of Login.gov's scale (over eighty-five million user accounts[85]) and significance ("[t]he public's one account for government"[86]), striking the balance between sometimes competing values is a difficult, but critically important task. In the words of Rashida Richardson and Amba Kak: "While certain efficiencies can be gained through digitized databases and data-driven analysis, these purported benefits must be evaluated and balanced with the risks and costs to society, along with whether their use or outcomes undermine governance goals or missions."[87] By treating LexisNexis as a quick fix to the challenge of verifying would-be Login.gov users, the team behind Login.gov forced unnecessary tradeoffs between the program's stated goals.

Just a few years exposed the weakness of this "quick fix" when an audit found that the Login.gov team had knowingly misrepresented

[84] Joel Minton, *Building a Modern Shared Authentication Platform*, 18F (May 10, 2016), https://18f.gsa.gov/2016/05/10/building-a-modern-shared-authentication-platform [https://perma.cc/E4TN-P6X5].

[85] Login.gov: Program Roadmap, *supra* note 6, at 7.

[86] Login.gov, https://login.gov [https://perma.cc/8MSY-GXVS].

[87] Rashida Richardson & Amba Kak, *Suspect Development Systems: Databasing Marginality and Enforcing Discipline*, 55 U. Mich. J.L. Reform 813, 879 (2022).

LexisNexis's capabilities.[88] In prioritizing expediency over community-involved design, the early Login.gov undermined its partners' and the public's trust in its capacity to serve as a useful digital infrastructure.[89]

A. *Login.gov's Precipitous Partnership with LexisNexis*

Login.gov's partnership with LexisNexis for identity verification was neither necessary nor a foregone conclusion. There are other ways to verify a user's identity. When it began developing Login.gov in 2016, the GSA stated that it was "looking at each and every technology component and deciding what to build, what to buy, and what to leverage from the open source community."[90] Login.gov could have used a biometric-based verification tool like the facial recognition technology employed by ID.me. Biometric identification is more difficult to defraud than record linkage, but is criticized for invading user privacy and for having lower accuracy for racial minorities.[91] Login.gov could have required in-person verification at post offices—an option it began to offer in October 2023.[92] In-person verification is both secure and data-minimizing, but requires training personnel across the country and requires people to leave the comfort of their homes to set up an account. Yet instead of weighing the benefits and drawbacks of these various options or soliciting input from the public, Login.gov quickly contracted with LexisNexis for "identity proofing" by algorithm.[93]

Around the same time that the GSA began developing Login.gov, the GSA also entered a multi-year schedule contract with LexisNexis.[94] The contract made LexisNexis's wide range of data intelligence, credit monitoring, auditing, fraud prevention, and financial management products available for purchase to agencies across the federal

[88] *See infra* Section II.B.

[89] *See* Press Release, U.S. House Comm. on Oversight & Accountability, Sessions: Login.gov Lied to Customers, Continued to Charge for Non-Existent Services (Mar. 29, 2023), https://oversight.house.gov/release/sessions-login-gov-lied-to-customers-continued-to-charge-for-non-existent-services [https://perma.cc/NX6C-2F5H].

[90] *Id.*

[91] *See, e.g.*, James Hendler, *Feds Are Increasing Use of Facial Recognition Systems – Despite Calls for a Moratorium*, Conversation (Sept. 1, 2021), https://theconversation.com/feds-are-increasing-use-of-facial-recognition-systems-despite-calls-for-a-moratorium-145913 [https://perma.cc/C4V7-782Y] [hereinafter Hendler Feds].

[92] *Login.gov Continues to Expand, Offering New Pathways to Securely Accessing Government Services Online*, *supra* note 58.

[93] LexisNexis PIA, *supra* note 14, at 6.

[94] *LexisNexis Special Services Inc. Awarded GSA Schedule Contract to Help Federal Agencies Fight Financial Fraud, Waste and Abuse*, PR Newswire (June 15, 2016), https://www.prnewswire.com/news-releases/lexisnexis-special-services-inc-awarded-gsa-schedule-contract-to-help-federal-agencies-fight-financial-fraud-waste-and-abuse-300285100.html [https://perma.cc/7D86-C3R4].

government.[95] Although this contract was not specifically about Login.gov or identity verification, it established a close working relationship between the data broker and the agency and laid the groundwork for future acquisitions.[96]

In 2017, the GSA posted a "Sources Sought Notice," essentially a market survey, asking for input from private sector identity verification providers about how Login.gov should build its verification service.[97] In the notice, the GSA said it was "highly interested in diverse approaches and data sources that can support this goal" and acknowledged "the need to have [a] mix of methods."[98] In January 2018, the GSA posted its first official solicitation for identity proofing contractors who could "resolve at least 50% of the U.S[.] population" and could verify user identities consistently with IAL2.[99]

A few months later, LexisNexis announced that it had won the Login.gov contract, stating: "Our public records data help fill in the gaps by providing additional support to help verify identity and help detect fraud."[100] Referring to the IAL system, the press release asserted that "LexisNexis technologies are fully compliant with NIST 800-level security standards"[101]—a false claim that would later land the GSA in hot water.[102] Although the GSA's solicitation is public, the responses to it are not, so it is difficult to tell how much competition there was for the contract or by what process LexisNexis was selected. I submitted a Freedom of Information Act (FOIA) request for this information, but have not received a response as of November 2024. The GSA's FOIA portal required me to sign in using Login.gov.

[95] *Id.*

[96] *Id.*

[97] *Technology Transformation Services Sources Sought Notice*, General Services Administration (Nov. 15, 2017), https://sam.gov/opp/17c48be921bd556beadbc3e22de03049/view [https://perma.cc/5ZYD-N62A].

[98] *Id.* Note that I submitted a FOIA request for the responses to this Notice, but as of April 6, 2024, I have not received any responsive documents.

[99] *Request for Quotes: Identity Proofing Blanket Purchase Agreements*, Gen. Servs. Admin. (Jan. 29, 2018), https://sam.gov/opp/4a61ebb3be04ad49fed68ca55a4bad89/view [https://perma.cc/T687-RXAZ]. Recall that IAL2 requires a biometric or in-person verification. *See supra* Section I.B.2. In this context, resolution refers to the process of "accurately identify[ing] the single, unique individual that the identity represents." Alison Hillendahl, *The Ultimate Guide to Identity Proofing*, Experian (Mar. 13, 2023), https://www.experian.com/blogs/insights/ultimate-guide-identity-proofing [https://perma.cc/EGU4-8HVR].

[100] *Spear and LexisNexis Risk Solutions Team to Expand and Strengthen Secure Access to Government Agencies Through the Login.gov Single Sign-on Solution*, LexisNexis Risk Solutions (Sept. 12, 2018), https://risk.lexisnexis.com/about-us/press-room/press-release/20180912-single-sign-on [https://perma.cc/2BGU-SBV2].

[101] *Id.*

[102] *See infra* Section II.B.

The partnership with LexisNexis solved a key challenge facing Login.gov: The platform needed a verification tool, and it wanted one as soon as possible. As the GSA explained just before LexisNexis announced the partnership, the agency needed a verification process that would be flexible enough to accommodate the hundreds of types of valid photo IDs that Americans use to prove up their legal identities.[103] With its database of over eighty-four billion public records and its SALT record linkage algorithm, LexisNexis provided a readymade solution to this problem. And time was of the essence. By 2018, there was a quickly growing market of private sector digital identity tools.[104] And several states had begun developing independent Digital ID platforms.[105] Login.gov needed to act quickly if it wanted to meet its stated goal of becoming the sole sign-on service for all government resources.

LexisNexis's record-linkage verification process proved to be a great asset in Login.gov's efforts to beat out verification competitors. In November 2021, the Internal Revenue Service (IRS) announced an $86 million contract with the private sector identity verification company ID.me.[106] The stated goal of the partnership was to reduce identity theft and increase security for citizens who wanted to pay their taxes online by requiring taxpayers to verify their identities with ID.me beginning

[103] Jon Prisby, *How Login.gov Used Evidence-Based Buying to Find Identity Proofing Software*, 18F (Aug. 7, 2018), https://18f.gsa.gov/2018/08/07/how-login-used-evidence-based-buying [https://perma.cc/72RA-RD7M] ("There are hundreds of types of valid photo IDs between the number of photo ID issuers (states, territories, federal government, tribes, etc.). The diversity of photo IDs and how they can be verified, such as by taking a photo/video or wirelessly for IDs that have a chip, meant we needed to take a flexible approach.").

[104] *See, e.g.*, ID.me, https://www.id.me [https://perma.cc/2UZR-K8LA]. Founded in 2013, ID.me won its first government contract in 2016. *See* James Hendler, *Why the Prospect of the IRS Using Facial Recognition Is So Alarming*, Slate (Feb. 2, 2022), https://slate.com/technology/2022/02/irs-id-me-facial-recognition.html [https://perma.cc/4ZMG-2ZHW] [hereinafter Hendler IRS].

[105] *See, e.g.*, OHID, https://ohid.ohio.gov/wps/portal/gov/ohid/home/home [https://perma.cc/G62N-GMEG] (Ohio); *Digital Identity Project*, Cal. Dep't of Tech., https://cdt.ca.gov/digitalID [https://perma.cc/JJR7-MUAA] (California).

[106] *See IRS Unveils New Online Identity Verification Process for Accessing Self-Help Tools*, IRS (Nov. 17, 2021), https://www.irs.gov/newsroom/irs-unveils-new-online-identity-verification-process-for-accessing-self-help-tools [https://perma.cc/R4HH-SVCU] (announcing the contract); Drew Harwell, *Huge Government Agencies Clash Over Imposing Facial Recognition*, Wash. Post (Feb. 7, 2022), https://www.washingtonpost.com/technology/2022/02/07/irs-gsa-id-facial-recogntion [https://perma.cc/PV5Y-MK2H] [hereinafter Harwell Facial Recognition] (reporting the contract's $86 million value). According to news reports, the U.S. Department of Veterans Affairs and the Social Security Administration were both also using ID.me at the time. *See* Joy Buolamwini, *The IRS Should Stop Using Facial Recognition*, Atlantic (Jan. 27, 2022), https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386 [https://perma.cc/CU7G-HW62].

in summer 2022.[107] But the IRS's decision to partner with ID.me drew a swift and furious backlash from critics who saw the partnership as a drastic impingement on civil liberties.[108] This firestorm opened a window for Login.gov to swoop in and win the high-profile contract.

People were incensed that the IRS would partner with ID.me, whose verification process utilizes facial recognition.[109] For one thing, facial recognition algorithms have historically had higher error rates when verifying Black or Asian faces relative to white faces, a result of biased training data.[110] For another, it was not clear whether ID.me was using a "one-to-one" matching algorithm, which compares only the selfie and the ID card, or a less trustworthy "one-to-many" matching algorithm, which would compare both photos against some larger, unspecified, and unreviewable database of photos that could perpetuate bias through over-inclusion or exclusion.[111] Moreover, privacy and algorithmic justice advocates loudly objected to any verification system that involves collecting and storing people's biometric data.[112] Over twenty members of Congress called for the IRS to cancel the contract.[113] Senator Ron Wyden wrote to the IRS Commissioner that "Americans should not

[107] *IRS Unveils New Online Identity Verification Process for Accessing Self-Help Tools*, *supra* note 106.

[108] *See* Drew Harwell, *IRS Plan to Scan Your Face Prompts Anger in Congress, Confusion Among Taxpayers*, Wash. Post (Jan. 28, 2022), https://www.washingtonpost.com/technology/2022/01/27/irs-face-scans [https://perma.cc/MR9N-98XZ] [hereinafter Harwell IRS Scan].

[109] *See Verifying Your Identity with Self-Service*, ID.me Help Ctr., https://help.id.me/hc/en-us/articles/4408234222871-How-do-I-verify-my-identity-using-my-ID [https://perma.cc/2S3E-4HZF].

[110] *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2023), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/YZ8E-CAX3].

[111] Buolamwini, *supra* note 106. One-to-many matching is often much more problematic, e.g., in the context of matching CCTV footage of a robbery against a database of mugshots.

[112] Hendler IRS, *supra* note 104.

[113] *See* Harwell Facial Recognition, *supra* note 106; *see also* Letter from Sen. Jeffrey Merkley & Sen. Roy Blunt to IRS Comm'r Charles Rettig (Feb. 3, 2022), https://www.merkley.senate.gov/senators-merkley-and-blunt-demand-the-immediate-halt-of-any-internal-revenue-services-irs-programs-using-american-taxpayers-biometric-data [https://perma.cc/35ES-XPFZ] (encouraging a ban on IRS use of biometric data collection); Letter from Sen. Mike Crapo et al. to IRS Comm'r Charles P. Rettig (Feb. 3, 2022), https://www.finance.senate.gov/imo/media/doc/id_me_letter_to_rettig.pdf [https://perma.cc/TF6S-88ZC] (raising concerns about ID.me compromising access to civil liberties and privacy); Press Release, U.S. S. Comm. on Com., Sci., & Transp., Wicker Questions IRS Security System Requiring Taxpayers to Submit Video Selfie (Feb. 3, 2022), https://www.commerce.senate.gov/2022/2/wicker-questions-irs-security-system-requiring-taxpayers-to-submit-video-selfie [https://perma.cc/Y42G-432R] (explaining security concerns and seeking additional information about the ID.me partnership).

have to sacrifice their privacy for security," and urged the agency to contract instead with Login.gov.[114]

As a result of the intense anti-facial recognition pressure, the IRS announced in February 2022 that it would abandon its partnership with ID.me.[115] That same day, the director of the GSA's Technology Transformation Services released a statement pronouncing the agency's commitment to not using facial recognition technology for Login.gov.[116] Within two weeks, the IRS announced that it would work towards a partnership with Login.gov, which at that point was still an underdeveloped platform with more indeterminate privacy and equity pitfalls.[117]

As it turned out, Login.gov's verification technology—that is to say, LexisNexis's record linkage algorithm—could not deliver on its promises. At the urging of the Department of the Treasury, the GSA, and the White House, the IRS spent two years working to try to implement Login.gov.[118] But the platform kept failing the IRS's security standards for identity verification.[119] In May 2023, the beleaguered IRS cancelled almost all of its $22.6 million contract with Login.gov.[120] This story is detailed in the next Section. It highlights the GSA's misguided and misleading efforts to fix the problems that it created by quickly contracting with LexisNexis instead of using a design and procurement process that properly considered the social and legal functions of Login.gov. However, it is equally important to remember that even though Login.gov lost the IRS contract, it maintains contracts with forty-eight agencies and states.[121]

[114] Letter from Sen. Ron Wyden to IRS Comm'r Charles P. Rettig (Feb. 7, 2022), https://www.finance.senate.gov/imo/media/doc/Wyden%20irs%20id%20me%20letter.pdf [https://perma.cc/LBB9-E6EX].

[115] *See* Press Release, IRS, IRS Announces Transition away from Use of Third-Party Verification Involving Facial Recognition (Feb. 7, 2022), https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition [https://perma.cc/9HYB-V26K]; *see also* Harwell Facial Recognition, *supra* note 106 (explaining that the IRS abandoned the planned contract due to the lack of regulation of facial recognition systems and the lack of accuracy for people of color).

[116] *See* Harwell Facial Recognition, *supra* note 106.

[117] Press Release, IRS, IRS Statement—New Features Put in Place for IRS Online Account Registration; Process Strengthened to Ensure Privacy and Security (Feb. 21, 2022), https://www.irs.gov/newsroom/irs-statement-new-features-put-in-place-for-irs-online-account-registration-process-strengthened-to-ensure-privacy-and-security [https://perma.cc/HTW2-VLGV].

[118] Treasury Inspector Gen. for Tax Admin., U.S. Dep't of the Treasury, Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification 4 (Sept. 27, 2023).

[119] *Id.*; *see also infra* Section II.B.

[120] Treasury Inspector Gen. for Tax Admin., *supra* note 118, at 16.

[121] Login.gov: Program Roadmap, *supra* note 6, at 7.

B. Login.gov's False Promises of a Secure and Equitable Digital ID

Login.gov's unsuccessful IRS contract is only one example of how the platform's partnership with LexisNexis has failed—and even undermined—other agencies' security requirements. In March 2023, the GSA's Office of Inspector General (OIG) released a report accusing the GSA's "18F" group, the subdivision responsible for developing Login.gov, of misleading its partners, funders, and the public about Login.gov's verification capabilities.[122] According to the OIG Report, 18F knowingly violated security requirements set by the National Institute for Standards and Technology and repeatedly lied about its noncompliance, thus defrauding partner agencies to the tune of $10 million.[123] The OIG Report describes an agency so eager to build Login.gov's cadre of partner agencies, and so determined to differentiate itself from unpopular facial recognition ID tools like ID.me, that it willingly risked the security of the nation's nascent Digital ID infrastructure.[124] Moreover, although LexisNexis helped the GSA skirt the objections to facial recognition, its record-linkage verification bears significant equity risks of its own.

The OIG Report revolves around Login.gov's false contentions that its verification technology complied with the National Institute for Standards and Technology's "Digital Identity Guidelines."[125] Released just two months after the GSA launched Login.gov, the Guidelines set forth technical requirements for digital identity tools deployed by federal agencies.[126] They include four volumes: one set of general guidelines, and volumes specific to "Enrollment and Identity Proofing," "Authentication and Lifecycle Management," and "Federation and Assertions."[127] Since May 2019, compliance with the Guidelines is mandatory for all federal agencies who implement digital identity verification, authentication, or both.[128]

[122] Off. of Inspector Gen., Gen. Servs. Admin., Off. of Inspections, GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards (Mar. 7, 2023) [hereinafter OIG Report].

[123] *Id.* at 1, 4.

[124] *Id.* at 21.

[125] *See* Digital Identity Guidelines, *supra* note 80.

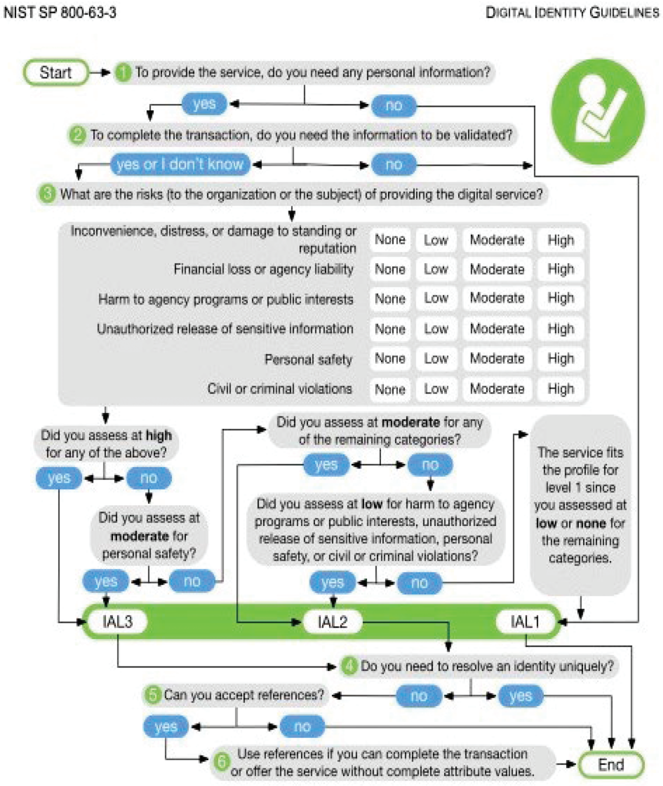
[126] *Id.* at iii. The Guidelines are issued pursuant to the Federal Information Security Modernization Act (FISMA), a 2014 law that primarily aims to secure federal information systems against cyber attacks. 44 U.S.C. § 3551 *et seq.*, Pub. L. No. 113-283.

[127] *See NIST Special Publication 800-63 Digital Identity Guidelines*, NIST, https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines [https://perma.cc/K4VZ-K784].

[128] Memorandum from the Acting Dir. of the Off. of Mgmt. and Budget on Enabling Mission Delivery through Improved Identity, Credential, and Access Management 2

The Digital Identity Guidelines aim to protect the privacy and security of both digital identity subjects and the organizations that rely upon digital identity credentials.[129] They define digital identity as "the unique representation of a subject engaged in an online transaction," and do not require that a digital identity be able to "uniquely identify the subject in all contexts."[130] They do, however, require federal agencies to assess the security and privacy risks associated with the resources they offer and to implement only those digital identity tools that meet an Identity Assurance Level (IAL) sufficient to mitigate those risks.[131] The process for determining which IAL is required for a given digital identity implementation is depicted in Figure 1.

FIGURE 1. IAL SELECTION


NIST SP 800-63-3
DIGITAL IDENTITY GUIDELINES
Start
1 To provide the service, do you need any personal information?
yes
no
2 To complete the transaction, do you need the information to be validated?
yes or I don't know
no
3 What are the risks (to the organization or the subject) of providing the digital service?
Inconvenience, distress, or damage to standing or reputation
Financial loss or agency liability
Harm to agency programs or public interests
Unauthorized release of sensitive information
Personal safety
Civil or criminal violations
None
Low
Moderate
High
Did you assess at high for any of the above?
yes
no
Did you assess at moderate for personal safety?
yes
no
Did you assess at moderate for any of the remaining categories?
yes
no
Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
yes
no
The service fits the profile for level 1 since you assessed at low or none for the remaining categories.
IAL3
IAL2
IAL1
4 Do you need to resolve an identity uniquely?
no
yes
5 Can you accept references?
yes
no
6 Use references if you can complete the transaction or offer the service without complete attribute values.
End

(May 21, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf [https://perma.cc/K8BZ-ZY8L].

[129] *See* DIGITAL IDENTITY GUIDELINES, *supra* note 80, at 28–29.

[130] *Id.* at iv.

[131] *See id.* at 18.

This complicated flowchart from the Guidelines instructs agencies on how to determine which IAL corresponds with the risks of their intended Digital ID implementation.[132]

In 2019, the GSA began advertising and billing Login.gov's partner agencies for IAL2-compliant verification services.[133] IAL2-compliant verification was an essential selling point for agencies with sensitive resources, such as the IRS and several others interviewed in the OIG Report.[134]

But, as the OIG Report found, Login.gov *never* met the IAL2 requirements.[135] For IAL2 compliance, the NIST guidelines require either a physical comparison or a biometric comparison of the applicant to "the strongest piece of evidence provided."[136] An IAL2 verification can be done in person, remotely via supervised video conference, or remotely via biometric comparison.[137] A satisfactory biometric comparison measures both biological characteristics (such as facial recognition) and behavioral characteristics (such as mousepad tracking).[138] Login.gov's method for verifying identities via LexisNexis's public record linkage algorithm does not employ any physical or biometric comparisons, and so does not satisfy IAL2.[139]

The OIG Report details how senior officials at Login.gov were repeatedly notified of Login.gov's noncompliance with the Digital Identity Guidelines, yet refused to change their verification process or correct their misrepresentations to partner agencies and funders.[140] According to internal messages quoted in the OIG Report, Login.gov's leadership framed this noncompliance as a simple values tradeoff between security and equity. During the summer of 2021, a high-level Login.gov official internally wrote that biometrics should not be used for verification because the discriminatory impact outweighs

[132] *Id.* at 27.

[133] *See* OIG Report, *supra* note 122, at 17.

[134] *See id.* at 15.

[135] *Id.* at 6.

[136] *Id.* at 3–4; *see also* Digital Identity Guidelines: Enrollment and Identity Proofing, *supra* note 52, § 5.3.1.

[137] *See* Digital Identity Guidelines: Enrollment and Identity Proofing, *supra* note 52, § 4.4.1.

[138] Digital Identity Guidelines, *supra* note 80, at 43.

[139] *See* OIG Report, *supra* note 122, at 4 ("[D]espite assertions . . . that they met SP 800-63-3, Login.gov has never included either a physical comparison or biometric comparison available to customer agencies, as required for identity verification at the IAL2 level. . . . Login.gov was instead using a third party to compare identification cards to information contained in LexisNexis.").

[140] *See generally* OIG Report, *supra* note 122.

the security benefits.[141] But the GSA did not notify its partner agencies about this position until January 2022, when the agency released an Equity Action Plan that vowed not to use biometric comparison technologies "until rigorous review has given us confidence that they can be implemented equitably."[142] And even then, it did not notify the eighteen agencies that had contracted for IAL2 verification services that Login.gov had *never* been IAL2-compliant.[143]

Moreover, nothing about LexisNexis's verification process is inherently more equitable than biometric comparisons. For one thing, the Login.gov-LexisNexis partnership entrenches the data broker industry, a $319 billion surveillance economy that goes largely unregulated and gives law enforcement access to surveillance data they could never collect alone.[144] For another, the SALT record linkage algorithm's reliance on scraping business, consumer, and social media records from across the internet means that people without a credit history or those who are new to the country are less likely to be correctly verified by LexisNexis. Finally, LexisNexis gets things wrong all the time, but provides no meaningful redress mechanism to people whom it misidentifies.[145]

[141] *Id.* at 12 ("The position of TTS is that the benefits of liveness/selfie does not outweigh any discriminatory impact, and therefore should not be used as a proofing requirement.").

[142] GSA, Equity Action Plan 10 (Jan. 20, 2022), https://www.gsa.gov/system/files/GSAEquityPlan_EO13985_2022.pdf [https://perma.cc/59VF-NJVY]. This Equity Action Plan was mandated by the Biden Administration. Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, Exec. Order No. 14,091, 88 Fed. Reg. 10825 (Feb. 16, 2023).

[143] *See* OIG Report, *supra* note 122, at 14–16 (showing that this lack of information gave some agencies the misimpression that the January 2022 announcement marked a change in policy.) *Id.*

[144] Devan Burris, *How Grocery Stores Are Becoming Data Brokers*, CNBC (Dec. 10, 2023), https://www.cnbc.com/2023/12/10/how-grocery-stores-are-becoming-data-brokers.html [https://perma.cc/E2AW-AW77] (reporting that in 2021, the data broker industry was worth $319 billion). For a discussion of data brokers' problematic and racially fraught role in policing, see Sarah Lamdan, *Revisiting the Privacy Act of 1974 for Big Data Policing*, 6 Geo. L. Tech. Rev. 386 (2022).

[145] After the OIG Report came out, the GSA launched an equity study on remote identity proofing. The report will "present a statistical analysis of failures and successes for the proofing checks and explore the causes behind negative or inconclusive results." *Questions About the Equity Study on Remote Identity Proofing*, U.S. Gen. Servs. Admin., https://www.gsa.gov/governmentwide-initiatives/diversity-equity-inclusion-and-accessibility/equity-study-on-remote-identity-proofing/questions-about-the-equity-study-on-remote-identity-proofing [https://perma.cc/J89Q-Y732]. This study represents progress towards building a digital identity infrastructure that takes the problem of false negatives (people being wrongly denied access to government benefits) as seriously as it takes the problem of false positives (successful fraud). However, as I argue in Part III, *infra*, such studies and their results must be part of a democratic conversation about infrastructure projects before they're built, not after the agency gets in trouble.

As explained in Part I, LexisNexis verifies a Login.gov applicant's identity by linking records from across the internet to evaluate whether the applicant's proffered identifying information matches LexisNexis's collection of records about the person she claims to be.[146] But people without access to computers or typical consumer profiles are less likely to have robust records for the linkage algorithm to process.[147] Immigrants, people with disabilities, and poor people—all groups with important claims to government benefits—may well be less likely to "engage in activities that big data and advanced analytics are designed to capture."[148] Therefore, in a system where the match threshold is based on an assumption that people have engaged in those activities, people who have not will be disproportionately denied Login.gov accounts.[149] On the other hand, given that the algorithm screens for "risk indicators," people from over-policed communities may be more likely to have data that might raise a flag.[150] And it can be difficult or impossible for a Login.gov user to determine what records form the basis for an exclusionary verification result.

In 2014, a man named Abraham A. Abdallah was denied a mortgage based on erroneous information in a report LexisNexis had provided to his bank.[151] The LexisNexis report was filled with "incorrect information, misspelled and incorrect names, and incorrect addresses and phone numbers."[152] In Abdallah's case, part of the problem appears to have been that his first and last names are common, making it more

[146] *See supra* Section I.B.

[147] *See* Mary Madden, Michele Gilman, Karen Levy & Alice Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash. U. L. Rev. 53, 65 (2017) ("[B]ig data can also result in the exclusion of marginalized groups from desirable opportunities 'because they are less involved in the formal economy and its data-generating activities [or because they] have unequal access to . . . the technology necessary to engage online, or are less profitable customers or important constituents . . . .'") (quoting Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016)).

[148] Jonas Lerman, *Big Data and Its Exclusions*, 66 Stan. L. Rev. Online 55, 56 (2013).

[149] *See* David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey & Mariano-Florentino Cuéllar, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies, Report Submitted to the Administrative Conference of the United States 79 (2020) ("In the presence of underlying differences between demographic groups, for instance, it is not possible to simultaneously equalize false positive rates, false negative rates, and predictive parity across groups.").

[150] *See id.* (presenting the example of an AI screening tool for child welfare services that scans records from means-tested welfare programs that exist for poor people, but not wealthy people, making poor people more likely to be flagged as "high risk").

[151] Abdallah v. LexisNexis Risk Sols. FL, Inc., 2021 WL 1209419, at *1 (E.D.N.Y., Mar. 30, 2021).

[152] *Id.*

difficult for LexisNexis's SALT algorithm to distinguish him from people with similar names. For example, one of LexisNexis's reports listed a previous address for him as "a jail cell in the Riker's [sic] Island adolescent unit," when the person who had actually been in Rikers was "a different individual, Abrihim A. Abdallah."[153] Although there is no public data about error rates, Abdallah's story suggests that people with common—or commonly misspelled—names are more likely to have inaccurate LexisNexis reports. If true, it follows that they would be more likely to be denied a Login.gov account based on erroneous verification.[154]

In addition to LexisNexis's substantive equity deficiencies, there are also few options for correcting verifications gone wrong. When Abdallah contacted LexisNexis to correct the report, it told him the information was an accurate reflection of data it obtained from the credit bureaus Equifax, Experian, and TransUnion, and that he should deal directly with them.[155] But when Abdallah contacted the credit bureaus, he found no mistakes in their reports.[156] Despite persistent efforts by Abdallah, LexisNexis repeatedly refused to correct his file, telling him that it was under no legal obligation to do so.[157] In 2016, Citibank closed nine accounts held by Abdallah and his wife, and Bank of America closed three.[158] Abdallah continued to file dispute reports with LexisNexis throughout 2016, 2017, and 2018, but LexisNexis continued to deny responsibility for the inaccuracies.[159] Left with no other options, Abdallah filed suit in federal court in June 2019, and litigated the case for nearly four years before LexisNexis settled in April 2023 and corrected the reports.[160] Abdallah is one of many people who have resorted to litigation in order to resolve disruptive and even disastrous inaccuracies in LexisNexis's records about them.[161]

[153] *Id.* at *2.

[154] This is an equity issue, too. According to the 2010 U.S. census, of the 21,747,473 people with the twenty most common last names, 65% were non-white. Only 49% of the census population was non-white. *See Frequently Occurring Surnames from the 2010 Census.*

[155] *Abdallah*, 2021 WL 1209419, at *1.

[156] *Id.*

[157] *Id.* at *2.

[158] *Id.* at *3.

[159] *Id.*

[160] *Id.* at *8. On March 30, 2021, the district court denied LexisNexis's motion to dismiss, finding that Abdallah had alleged enough facts to "plausibly state a claim for willful failure to reinvestigate or delete incorrect information, in violation of [15] U.S.C. § 1681i(a) and N.Y. Gen. Bus. Law § 380-f."

[161] *See also, e.g.*, Reimer v. LexisNexis Risk Sols., Inc., No. 22-cv-153, 2022 WL 4227231, at *1–3 (E.D. Va. Sept. 13, 2022) (describing the plaintiff's unsuccessful two-year attempt to correct mistakes in his LexisNexis report before resorting to litigation); Fears v. LexisNexis Risk Sols., Inc., No. 19-2558, 2020 WL 12950811, at *1–2 (D. Minn. Aug. 12, 2020) (describing

Login.gov users who are wrongly denied an account at the verification stage have the option of pursuing Abdallah's nine-year litigation strategy to force LexisNexis to correct their file. They also have the option of mailing a Request to Amend Record to Login.gov's system manager.[162] Under the Privacy Act of 1974, individuals may request to have agency records about them amended, and the agency is required to provide an explanation if the amendment request is denied.[163] However, the Digital Identity Guidelines prohibit Digital ID providers from giving an explanation for a failed identity proofing attempt, fearing that such explanations will help future fraudsters to access records illegally.[164] Moreover, no procedural recourse can make up for a system that unfairly excludes people in the first instance. Instead, "any due process regime [must] ensure that low-income people have a voice in designing systems for transparency and accountability, that their interests are represented by enforcement entities, and that enforcement involves systemic review of algorithmic processes rather than reliance on individual complaints."[165]

As presented in the OIG Report, Login.gov's fraud debacle is a dramatic tale of two warring agencies, one committed to security and the other to equity. But this is a false choice: Both must be essential priorities for any functional digital identity infrastructure, yet Login.gov's development process achieved neither. In reality, 18F's "start-up mentality" led the GSA to rush into a partnership with LexisNexis—disregarding the company's intrusive and careless business practices—in an effort to win customers and achieve cost recovery without taking time to think through the best way forward.[166]

the plaintiff's failed attempts to correct mistakes in his LexisNexis report, which had resulted in his being denied a home loan); Jones v. LexisNexis Risk Sols., Inc., No. 20-cv-02496, 2021 WL 3269638, at *1–2 (D. Colo. July 30, 2021) (describing the plaintiff's frustrated efforts to amend mistakes in his LexisNexis report, which had resulted in his being prevented from purchasing a phone at a T-Mobile store).

[162] Privacy Act of 1974, 5 U.S.C. § 552a; Notice of a Modified System of Records, 87 Fed. Reg. 70819, 70822 (Nov. 21, 2022); *see also* 41 C.F.R. § 105-64.4 (2023).

[163] 41 C.F.R. § 105-64.4 (2023).

[164] Digital Identity Guidelines: Enrollment and Identity Proofing, *supra* note 52, at § 8.4.

[165] Madden et al., *supra* note 147, at 120 (alteration in original) (writing that procedural reforms risk a "masking of systemic injustice through the framework of individual fair hearings").

[166] OIG Report, *supra* note 122, at 21. *See also* Off. of Inspections and Forensic Auditing: Off. of Inspector Gen.: U.S. Gen. Servs. Admin., Evaluation of 18F (Oct. 24, 2016) (describing poor time management, improper execution of agreements, and incorrect billing at 18F); *see also* Off. of Inspections and Forensic Auditing Off. of Inspector Gen. U.S. Gen. Servs. Admin., Evaluation of 18F's Information Technology Security Compliance 1 (Feb. 21, 2017) (finding that 18F "routinely disregarded and circumvented fundamental security requirements").

III
Toward a Digital ID that Serves the Public Interest

In December 2022, Politico ran a story under the headline "Data Brokers Raise Privacy Concerns—But Get Millions From the Federal Government," which recognized Login.gov's contract with LexisNexis as a dubious but expedient workaround to the Privacy Act of 1974.[167] The story reports that the GSA was "reluctant" to use a data broker for verification, but didn't have "any viable alternatives."[168] It's true that LexisNexis's compilation of over eighty-four billion records is more comprehensive than anything the government could build for itself, as a matter of resources or as a matter of law under the Privacy Act.[169] This acquisition is legal under the Privacy Act. But the entrenchment of data brokers in digital infrastructure simply because they provide a simple, off the shelf service does violate the spirit, if not the letter, of the law.

The Congress that passed the Privacy Act of 1974 understood the importance of building trustworthy digital infrastructure. For this reason it enshrined principles of consent, redress, data minimization, security, transparency, and democratic participation in the Act. Unfortunately, instead of starting from these principles, the GSA built Login.gov on top of an existing infrastructure with opaque technologies, an extractive business model, and inadequate accountability mechanisms. Although the Privacy Act does little to protect individual privacy in the age of data brokers, it should still be used as a framework for building public information systems that operate in a trustworthy manner. Going forward, digital infrastructure projects should treat these as foundational design principles, not considerations to paper over after the infrastructure's failings are exposed. And government agencies should ensure that private contractors abide by the same principles, rather than treating public-private partnerships as a convenient workaround.

A. The Privacy Act Is Not the Answer . . . Or Is It?

The Privacy Act was written before there was any private industry with surveillance power anywhere near that of modern data brokers. A popular critique of the Privacy Act is that it imposes few substantive privacy protections, relying instead on procedural reporting

[167] Alfred Ng, *Data Brokers Raise Privacy Concerns—But Get Millions From the Federal Government*, Politico (Dec. 21, 2022), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600 [https://perma.cc/5LH6-VYME].

[168] *Id.*

[169] *See Search Public Records*, LexisNexis, https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page [https://perma.cc/2EFY-PM84] (boasting a database of over eighty-four billion records).

requirements, and that even its procedural protections are frustrated by a robust set of exceptions.[170] These reporting requirements apply to systems of records maintained by government agencies as well as government contractors like LexisNexis.[171] But the Privacy Act's few substantive constraints on data collection and sharing apply only to data collected directly by federal agencies, not data acquired from third parties.[172] For these reasons, the Privacy Act has proved inept at reining in the federal government's ability to access the vast amounts of personal information available through data brokers.

In the context of the Login.gov contract, the Privacy Act required the GSA to publish a Systems of Records Notice alerting the public to the role of contractors in the platform.[173] The notice never mentions LexisNexis by name, referring only to "third-party identity proofing services."[174] Nor does the notice offer any explanation of how those third party identity proofing services operate or what records they consult on Login.gov's behalf.[175] And the Privacy Act's weak substantive protections make it perfectly allowable for the GSA to hire LexisNexis to do the dirty work of collecting, concatenating, and analyzing records to decide who will or won't gain access to government resources via Login.gov.

On the other hand, the Privacy Act enshrined a set of "Fair Information Practice Principles" that are as relevant today as they were in 1974. According to these principles, individual data subjects should consent to share their information and to every subsequent use of their records.[176] They should also be able to review and amend records held about them.[177] Federal agencies should practice data minimization; collect information directly from the individual; inform individuals of the purposes of data collection; develop and publicize rules of conduct for the design and maintenance of systems of records; ensure security and confidentiality; and solicit feedback and input from the public before putting a system of records to a new use.[178] As futile as its regulatory scheme may be in the age of data brokers, the Privacy

[170] *See* Bridget A. Fahey, *Data Federalism*, 135 Harv. L. Rev. 1007, 1037–39, n.133 (2022).

[171] 5 U.S.C. § 552a(m)(1).

[172] Fahey, *supra* note 170, at 1038.

[173] *See* Privacy Act of 1974, 5 U.S.C. § 552a; Notice of a Modified System of Records, 87 Fed. Reg. 70819, 70819–22 (Nov. 21, 2022) (describing Login.gov's collaboration with third party identity proofing services in the federal register, as required by the Privacy Act).

[174] *Id.* at 70819–20.

[175] *See id.*

[176] *See* 5 U.S.C. § 552a(b).

[177] *See id.* § 552a(d).

[178] *Id.* § 552a(e)(1)–(12).

Act contains significant wisdom on how a government ought to build systems of records that engender public trust.

It is no surprise that the Privacy Act's drafters drafted such a thoughtful set of principles for trustworthy digital infrastructure. In 1974, America was reeling from the Watergate and Counterintelligence Program scandals' revelation that the federal government was conducting illegal surveillance on political minorities and maintaining dossiers on "subversive" individuals.[179] At the same time, the government was experimenting with the earliest iterations of electronic databases and so confronting new questions about how the transition from paper files to computer-based recordkeeping would change ownership, privacy, and utility of information.[180] In an effort to rehabilitate public trust in the government while also preserving the utility of these new technologies, Congress passed the Privacy Act.[181] As then-Chairman of the Senate Judiciary Committee Sam Ervin stated in support of the Act: "If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens."[182]

Despite its name, the Privacy Act is really a trust in government law, not a data privacy law. The law was designed to bolster the public's trust in government in an increasingly digital age, not to protect individuals' privacy across the board. Because the Privacy Act is concerned only with government surveillance, nothing in the law prevents data brokers like LexisNexis from building enormous systems of public records or from selling that information to the government. But a data broker's business model is to build systems of records that look exactly like what the law's drafters aimed to prevent. Indeed, many of the records in LexisNexis's database are initially purchased from government actors.[183] For years, scholars, activists, and politicians have called for regulation

[179] U.S. Dep't of Just., Overview of the Privacy Act of 1974 1 (2020).

[180] *See id.* at 1 (describing how the Privacy Act was modeled off "the first comprehensive study of the risks to privacy presented by the increasingly widespread use of electronic information technologies by organizations," which developed "a 'code of fair information practices,' now more commonly called the Fair Information Practice Principles, or FIPPs").

[181] *See* The Privacy Act of 1974, Elec. Priv. Info. Ctr., https://epic.org/the-privacy-act-of-1974 [https://perma.cc/A8Y5-JJV4].

[182] U.S. Dep't of Just., *supra* note 179, at 1 (quoting S. Comm. on Gov't Operations & H.R. Comm. on Gov't Operations, 94th Cong., Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579) 4 (Comm. Print 1976)).

[183] *See* Lamdan, *supra* note 144, at 397 ("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."); 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/5RKM-98VS] (reporting that the state

of this industry, arguing that data brokers degrade personal privacy by piecing together disparate pieces of information to create, and sell, a comprehensive picture of any person's entire life.[184]

But as the call to regulate data brokers has grown louder, the data broker industry has intensified its lobbying push to kill legislation that would restrict its data collection practices. In June 2022, a bipartisan group of congressional representatives released a draft bill called the American Data Privacy and Protection Act (ADPPA), which could have been America's first comprehensive data privacy law.[185] That same quarter, data brokers spent $1.73 million on lobbying.[186] The data broker with the largest lobbying expenditures was RELX, LexisNexis's parent corporation.[187] The ADPPA never made it to the Senate. Government partnerships with unregulated surveillance contractors like LexisNexis can erode the trust in government that the Privacy Act was designed to bolster. And by entrenching data brokers in government infrastructure via multimillion dollar contracts, this type of public-private partnership further insulates this surveillance apparatus against regulation.

However, even if Congress could pass a new data privacy law, "privacy" alone will never ensure that digital infrastructure truly serves the public interest. What we need is trustworthy infrastructure designed based on community priorities. This is exactly what the Privacy Act of 1974 aimed to achieve by enshrining the principles of informed consent, redress, data minimization, transparency, security, and democratic participation. Even as Congress tries and fails to pass new privacy laws, the government is neglecting important principles established in this law from fifty years ago. Despite its implementation failures to date, the Privacy Act provides an important framework for governing the federal government's infrastructure in the digital age.

of Washington made $26,371,232 in one year selling DMV records to data brokers including LexisNexis).

[184] *See, e.g.*, Chris Jay 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 (2004) (arguing that the Privacy Act of 1974 should apply to commercial data brokers); Press Release, Federal Trade Commission, *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control over Their Personal Information* (May 27, 2014) (recommending federal legislation to make data brokers more transparent and accountable); Press Release, Sen. Elizabeth Warren, *Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers from Selling Americans' Location and Health Data* (June 15, 2022) (announcing the Health and Location Data Protection Act, which would ban data brokers from selling certain sensitive data).

[185] H.R. 8152, 117th Cong. (2022).

[186] Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, Politico (Aug. 28, 2022), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958 [https://perma.cc/QL5K-N4JB].

[187] *See id.*

B. Building Trustworthy Digital ID Infrastructure

The Privacy Act's fair information practice principles provide a useful foundation upon which Login.gov or any other Digital ID infrastructure is built. Digital ID may not be the best way, or even a good way, of distributing government resources in every scenario. But as long as the government is committed to building a Digital ID project, it needs to ensure that Digital ID platforms serve the public's interest in a reliable, safe, non-punitive, and equitable way to access government resources online. This will require a slower, more participatory building project. This Section makes some suggestions for how this could work.

1. Purpose-Specific Consent

As an initial matter, Digital ID platforms must be based on purpose-specific consent. Although the platforms should also seek to minimize the personal data they collect and retain, discussed below, some data collection will be necessary for effective digital infrastructure. One key to establishing trust in these systems is ensuring that people understand how their data is being used, and consent to that use. Professor Helen Nissenbaum's theory of contextual integrity proposes a compelling vision of this concept.[188] She writes that cause for alarm arises when information technologies violate people's expectations about the balance of power and flow of information in society.[189] Data shared for one purpose cannot be treated as automatically available for any other purpose because it carries an entirely new significance when combined with other pieces of information and when in the hands of recipients with different powers and authorities.[190] Under this model, the entrenchment of data brokers like LexisNexis—which sweep the internet for records, aggregate them, and then use the compiled package to analyze specific attributes of a person's identity—is highly problematic.

2. Redress

Login.gov's FAQ and the Digital Identity Guidelines only briefly mention redress in the event of a verification gone wrong.[191] The guidelines state that a Content Service Provider (CSP) must provide

[188] *See generally* Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (2009).

[189] *Id.* at 3–4, 186.

[190] *See id.* at 216.

[191] *See* Digital Identity Guidelines: Enrollment and Identity Proofing, *supra* note 52, §§ 4.2.5, 8.4; *see also* Nat'l Inst. of Standards and Tech., Digital Identity Guidelines: Enrollment and Identity Proofing (Dec. 2022), https://doi.org/10.6028/NIST.SP.800-63A-4.ipd [https://perma.cc/DMG3-F6PJ] (new draft guidelines).

a mechanism for redress of digital identity applicants' complaints or problems, and that for federal CSPs (like Login.gov) the instructions for redress must be provided in a Systems of Records Notice (SORN) pursuant to the Privacy Act of 1974.[192] This is effectively a bare minimum redress provision, as it merely restates the requirements of the Privacy Act, which provides that an individual may request access to records about them in a federal system of records.[193] An individual who is denied access and wishes to appeal that denial may file an appeal with the GSA, which can take months or years to fully litigate.[194]

Digital ID infrastructure ought to build above these bare minimum redress requirements by requiring simpler, more automatic means of seeking redress and alternative identity proofing options to people who have been wrongly excluded. And instead of leaving it to individuals to flag and correct false negatives, Digital ID should aim for "accountability by design."[195] Verification results should be regularly reviewed to ensure that error rates and associated demographic biases are documented and corrected.[196]

3. *Data Minimization*

Data-maximizing infrastructures are prone to abuse, especially by law enforcement. Time and again, technologies designed for banal, even useful, purposes have swelled the surveillance capacity of police and prosecutors. Subpoenas and search warrants for cell-site location information,[197] emails,[198] and Google Maps history[199] all exemplify this dynamic: If we build it, the cops will want to use it to surveil us. Inevitably, increased police surveillance is disproportionately directed at people of color, which puts these communities at even greater risk

[192] Digital Identity Guidelines: Enrollment and Identity Proofing, *supra* note 52, §§ 4.2.5, 8.4.

[193] 41 C.F.R. § 105-64.2 (2023).

[194] 41 C.F.R. §§ 105-64.303–105-64.305 (2023).

[195] *See* Engstrom et al., *supra* note 149, at 74 (citing Margot E. Kaminski, *Binary Governance: Lessons from GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 24, n.125).

[196] LexisNexis engineers even recommend this as best practice, although there is no indication online that Login.gov currently does this. *See* Middleton & Bayliss, *supra* note 64, at 222.

[197] *See* Carpenter v. United States, 585 U.S. 296 (2018) (holding that obtaining cell-site location information requires a warrant).

[198] *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that turning over emails to government agents requires a warrant).

[199] *See* United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (holding that a geofence warrant was invalid because it was overbroad).

of over-prosecution and police violence.[200] And fear of surveillance and its attendant punishment can lead people to avoid sharing information required to claim benefits, leading to exclusion and marginalization of communities with the most to fear.[201]

Digital ID tools raise particular concerns, as they are designed to be used in a vast array of circumstances, including every time a person wants to claim government benefits. These infrastructures therefore must be designed not to retain sensitive personal information. Moreover, the Digital ID tools should never allow the government to aggregate the data from a user's various transactions, as this can paint a comprehensive picture of a person's private information.[202] For example, cryptographic tools like Zero-Knowledge Proofs should be considered to ensure that data used for verification is only used for that limited purpose, and that only strictly necessary information is shared.[203] As a step in the right direction, Login.gov began offering in-person verification at U.S. Post Offices as an alternative to remote verification via LexisNexis.[204] But many millions of people will continue to opt for remote verification, so those processes must still be up to scratch in order to build a trustworthy and efficient national infrastructure.

4. *Security*

Greater flexibility in the process and results of the threat modeling would go a long way towards ensuring that the Digital Identity Guidelines' verification requirements align with the actual

[200] *See, e.g.*, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 348 (4th Cir. 2021) ("Too often today, liberty from governmental intrusion can be taken for granted in some neighborhoods, while others 'experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures.'").

[201] *See, e.g.*, Karen Hacker et al., *The Impact of Immigration and Customs Enforcement on Immigrant Health: Perceptions of Immigrants in Everett, Massachusetts, USA*, 73 Soc. Sci. & Med. 586, 591 (2011).

[202] *Cf.* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (writing that location data raises constitutional concerns because it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

[203] *See* W3, Verifiable Credentials Data Model v1.1: W3C Recommendation (Mar. 3, 2022) § 5.8, https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs [https://perma.cc/4NL5-KQH5] ("A zero-knowledge proof is a cryptographic method where an entity can prove to another entity that they know a certain value without disclosing the actual value.").

[204] *Login.gov Continues to Expand, Offering New Pathways to Securely Accessing Government Services Online*, GSA Blog (Oct. 18, 2023), https://www.gsa.gov/blog/2023/10/18/logingov-continues-to-expand-offering-new-pathways-to-securely-accessing-government-services-online [https://perma.cc/W59R-KPKY]. On the other hand, Login.gov simultaneously announced that it would be introducing verification via live video conference and verification via facial matching technology. *Id.*

risks associated with a given Digital ID implementation. At present, the Digital Identity Guidelines' process for the assessment is entirely hypothetical and self-contained within the implementing organization. The result of this assessment is to channel each use into one of the three IALs.[205] The Guidelines could introduce an "unacceptable risk" concept like the one in the EU's proposed Artificial Intelligence Act.[206] Such an addition could prohibit Digital ID implementations that bear an unknown risk of wrongful exclusion from critical welfare resources, such as identity verification via LexisNexis.

In general, the Guidelines would do better to focus on the security of digital identity infrastructure against large-scale attacks, rather than on individual risk scoring.[207] Identity theft is an important concern, but an overly zealous approach to one-off fraud risks cutting off swaths of people from needed benefits. In order to balance competing values, Digital ID tools could prohibit remote verification where the security risks are too high to forgo biometric comparisons, but the privacy or equity risks are too high to permit existing formats of biometric verification. This could push biometric verification tools to improve on privacy and equity, while forcing Digital ID providers and regulators to consider how their tools work and how they impact people before implementing them.

5. *Transparency & Democratic Participation*

When building digital infrastructure, government agencies must ensure that design, procurement, and evaluation processes are transparent and participatory. For example, there is no way for people outside LexisNexis to know how likely it is that a Login.gov applicant will be denied an account based on a LexisNexis misidentification. The E-Government Act of 2002 requires federal agencies to publish Privacy Impact Assessments ("PIAs"), reports that contain information about how the agency collects, uses, maintains, and shares electronic data that contains personal data.[208] The GSA published a PIA about the partnership between Login.gov and LexisNexis, but instead of

[205] *See supra* Figure 1 and accompanying text.

[206] Artificial Intelligence Act, Reg. (EU) 2021/0106, art. 5.2.2 (prohibiting the use of AI systems for manipulation of behavior, social scoring, or live biometric identification).

[207] Comments of the Electronic Privacy Information Center and the American Civil Liberties Union to the National Institute of Standards and Technology on Digital Identity Guidelines: Enrollment and Identity Proofing, Initial Public Draft (Apr. 14, 2023) (suggesting that "as a baseline rule, fraud prevention tools targeted at catching large scale attacks are less likely to harm individuals than tools for risk-scoring and back-end matching programs").

[208] E-Government Act of 2002, Public Law 107-347, § 208, 116 Stat. 2899, 2921 (2002).

explaining how the tools work, the PIA merely restates the aims of each of the LexisNexis tools used in the verification process.[209]

Public infrastructure should serve the public interest. There is no way of figuring out what that means without input from and accountability to the people the infrastructure is meant to serve. This means ensuring that all design and procurement procedures be open to public participation and comment. For example, public hearings could be required before the government enters into any contract that involves data collection for the purpose of distributing public benefits.[210] Transparency also means ensuring that any commercial vendors whose products are used in the infrastructure are held to the same standards of data governance as government actors would be. This includes constraints on data collection, aggregation, and retention; reporting requirements under the Privacy Act and the Freedom of Information Act; and susceptibility to litigation. When the government entrenches commercial vendors in public infrastructure, it is using taxpayer money to subsidize and empower corporations. The public should be able to evaluate and accept or reject those subsidies. Most importantly, trustworthy infrastructure means educating the public on how the technology works, what risks of error and exclusion are involved, how the government does and does not utilize the data it collects, and how to get help navigating it.

Conclusion

The troubled early history of Login.gov, America's first national Digital ID, is an illuminating case study of the promises and pitfalls of building digital public infrastructure. There is a great sense of urgency around the world to digitize public services and deliver benefits to people over the internet. This urgency is often presented as a dire need to expand access to government resources, especially in times of crisis like the COVID-19 pandemic. But in reality, the infamous "move fast and break things" mentality of the technology private sector is hardly

[209] LexisNexis PIA, *supra* note 14. For example, instead of explaining how the SALT algorithm handles record linkage, the PIA's explanation of its Emailage tool reads as follows: "Emailage assesses risk by evaluating email address metadata points such as domain details, email details, risk indicators, and when available, other personally identifiable information." *Id.* at 7.

[210] Pre-contract public hearings are not a radical idea. For example, the New York City Charter requires city agencies to hold such hearings "on proposed contracts valued in excess of $100,000 that are being awarded by a method other than competitive sealed bidding." *Public Hearing: Contract and FCRC Public Hearings Schedule, Agenda, and Calendar*, NYC Mayor's Office of Contract Services, https://www.nyc.gov/site/mocs/about/public-hearing.page [https://perma.cc/3XP4-CE6J].

the best way to build trustworthy government infrastructure. In the case of Login.gov, expediency led to agency infighting, fraud, and haphazard, misguided efforts to address equity concerns.

Instead of rushing out tech products that mirror or entrench dangerous private sector practices, digital public infrastructure projects should take as their starting point the fair information practice principles enshrined in the Privacy Act of 1974. The Privacy Act is understandably maligned for its feeble impact on personal privacy, especially given the ever-expanding role of data brokers like LexisNexis in government programs like Login.gov. But despite its regulatory inefficacy, the Privacy Act contains important lessons about building trust in government through data infrastructures centered on purpose-specific consent, redress, data minimization, security, transparency, and democratic participation.