NATIONAL ID FOR PUBLIC PURPOSE

Nathaniel Kim*

CITE AS: 7 GEO. L. TECH. REV. 272 (2023)

TABLE OF CONTENTS

I. INTRODUCTION

Starting on March 23, 2022, residents of Arizona could add a digital copy of their driver's license or state identification ("ID") to their Apple

* J.D. Class of 2024, Georgetown University Law Center. Many thanks to Professor Julie Cohen for her invaluable guidance and feedback in her seminar course, Technology Law and Policy Colloquium: Data, Algorithms, and Platforms. Thank you also to Professors Paul Ohm and Anupam Chander for their helpful comments.

Wallet, allowing them to use their iPhones or Apple Watches to present valid government identification at airport security checkpoints.[1] The state reported that over 11,000 people had requested digital copies of their Arizona IDs in the first 24 hours alone.[2] Apple is expecting to roll out similar driver's license projects in eleven states and Puerto Rico,[3] and Google is likely not far behind in supporting digital state IDs on Android smartphones.[4] With 85 percent of Americans owning a smartphone as of February 2021,[5] one can expect a similarly high adoption of mobile driver's licenses and digital state IDs in the next few years.

Though on the surface the ability to store and present official state IDs on one's smartphone seems to be just another added convenience in an increasingly digital world, this transition raises an important question about whether Americans are finally ready to embrace a national ID system. While digital state ID is certainly not the same thing as a national ID managed by the federal government, new capabilities enabled by the digital format (e.g., QR codes which reveal only pertinent information, like whether the owner is of legal drinking age[6]) and recent developments in the past two decades point to an American public that may be more open to a national ID regime.

First, states across the country have begun to issue IDs that meet the requirements of the REAL ID Act of 2005, which standardized the information included in state IDs as well as their authentication and issuance procedures.[7] Though originally proposed as part of a larger national security measure against terrorism,[8] the rollout of REAL IDs will, at minimum, establish new expectations for the federal government's involvement in managing IDs.

---

[1] Neil Vigdor, *Arizona Offers Driver's Licenses on iPhones. Other States Want to Be Next*. N.Y. TIMES (Mar. 26, 2022), https://www.nytimes.com/2022/03/26/us/arizona-digital-drivers-license.html [https://perma.cc/8EQQ-84FG].

[2] *Id*.

[3] *Id*.

[4] Chris Velazco, *Digital driver's licenses take the sting out of forgetting your wallet. Here's how they work*, WASH. POST (Oct. 11, 2021), https://www.washingtonpost.com/technology/2021/10/11/digital-drivers-license-mdl/ [https://perma.cc/DD5G-37GX] ("Google has been working to build support for verifiable electronic IDs into Android and teamed up with Apple and others to define a technical standard for how these IDs should work. The code for it technically already exists in Android 11 and 12, but the company hasn't announced plans to store digital state IDs in any of its apps yet.").

[5] *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/. [https://perma.cc/F3BT-REG9].

[6] Velazco, *supra* note 4.

[7] *About REAL ID*, U.S. DEP'T. HOMELAND SEC. (Dec. 16, 2021), https://www.dhs.gov/real-id/about-real-id [https://perma.cc/WNH2-73ZS]; REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231.

[8] *The History of Federal Requirements for State Issued Driver's Licenses and Identification Cards*, NAT'L CONF. STATE LEGISLATURES,

Second, the COVID-19 pandemic has presented a painful reminder that certain problems cannot be effectively addressed on a state-to-state basis. The pandemic has highlighted the need for a national ID system, both for improving public health surveillance as well as for empowering the federal government to efficiently distribute aid to eligible individuals.[9] As the pandemic raged on, more than 60 percent of Americans expressed their belief that the federal government should lead COVID-19 testing efforts,[10] and commentators have raised national IDs as a way to tackle increasing concerns about public health surveillance and cyber fraud.[11] Indeed, a poll conducted last year indicated that a majority of Americans favored the establishment of a national ID system.[12]

I argue that the United States should launch a national ID system as a substitute for the highly undesirable status quo we find ourselves in today:

---

https://www.ncsl.org/research/transportation/history-behind-the-real-id-act.aspx [https://perma.cc/S8T3-HAWV] (last visited Mar. 29, 2022).

[9] Howard K. Koh, *We need one response – not 50 – to fight Covid-19*, STAT (May 22, 2020), https://www.statnews.com/2020/05/22/we-need-one-response-to-fight-covid-19-not-50/ [https://perma.cc/ZWE2-ATCE] (emphasizing the need for stronger federal government leadership in pandemic response, especially in information collection efforts such as testing and contact tracing); Ian Kullgren, *IRS mistakenly sends stimulus checks to foreign workers*, POLITICO (May 1, 2020, 3:14 PM), https://www.politico.com/news/2020/05/01/irs-mistakenly-sends-stimulus-checks-to-foreign-workers-228974 [https://perma.cc/U3VW-75E4] (reporting that the IRS sent thousands of stimulus checks in error to foreign nationals). *See also* Ndiame Diop, *Transforming Social Protection Delivery in the Philippines through PhilSys*, WORLD BANK (Oct. 14, 2021), https://www.worldbank.org/en/news/opinion/2021/10/14/transforming-social-protection-delivery-in-the-philippines-through-philsys [https://perma.cc/MZ7G-JF6Z] (discussing the expected benefits of the Philippines' new national ID program in strengthened emergency subsidies delivery, financial inclusion efforts, and efficient vaccine distribution).

[10] *Most Americans Say Federal Government Has Primary Responsibility for COVID-19 Testing*, PEW RSCH. CTR (May 12, 2020), https://www.pewresearch.org/politics/2020/05/12/most-americans-say-federal-government-has-primary-responsibility-for-covid-19-testing/ [https://perma.cc/TQ25-297N] (reporting that "a majority of Americans (61 percent) say it is primarily the federal government's responsibility to make sure there are enough COVID-19 tests" to make decisions about stay-at-home restrictions).

[11] *See* Michael Segal, *America Needs a National Identity Card*, WALL ST. J. (Jan. 20, 2021, 6:01 PM), www.wsj.com/articles/america-needs-a-national-identity-card-11611183672 [https://perma.cc/YJ78-X6ZW]; Shai Cohen, *Could COVID-19 accelerate the adoption of a national digital ID in the US?* BIOMETRIC UPDATE (Jan. 11, 2021, 9:53 PM), https://www.biometricupdate.com/202101/could-covid-19-accelerate-the-adoption-of-a-national-digital-id-in-the-us [https://perma.cc/WH3R-TJEZ].

[12] While the poll was specifically focused on measuring respondents' opinions on the use of national ID for determining voter eligibility, its result nevertheless indicates Americans' openness to the idea of a national ID system. *See* Russell Berman, *The Obvious Voting-Rights Solution That No Democrat Will Propose*, THE ATLANTIC (Aug. 30, 2021), https://www.theatlantic.com/politics/archive/2021/08/voting-rights-national-id-card/619772/ ("51 percent of respondents favored a national ID that could be used for voting.").

Private actors compile dossiers of information on every consumer in the nation without meaningful consent, and third-party data brokers peddling that information to anyone willing to pay (including government agencies). None of it is used to benefit the public. The new national ID should be designed from conception for a pro-social purpose, with the aim of improving delivery of public benefits to the American people. The myriad benefits of a national ID regime include efficient administration of benefits and taxes, as well as accurate management of public records and census-taking. A national ID scheme can also be used for a variety of authorization and authentication needs, such as for forming contracts and verifying financial transactions. A securely implemented system would also mitigate risks of fraud, whether it be identity fraud, voter fraud, or benefit fraud.[13] Despite these potential benefits, the 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.[14]

There are, of course, good reasons to be concerned about national ID: ;section II identifies three common fears associated with national ID systems and considers examples of how prior failures have substantiated these fears. Section III discusses recent cryptographic and technological developments that have been successfully harnessed both here and abroad, suggesting a path forward for a national ID. Finally, section IV explains how the U.S. could learn from these successes and failures to establish a national ID system that is designed for public purpose.

.

II. FEARS AND FAILURES

National ID is frequently proposed as a solution for issues in national security, voter authentication, and immigration, but it has been ultimately rejected each time by critics in both political parties for reasons ranging from privacy concerns to illegitimate profiling.[15] Numerous arguments have been

[13] *See* Philip Redfern, *Precise Identification Through a Multi-Purpose Personal Number Protects Privacy*, 1 INT'L J.L. & INFO. TECH. 305, 312 (1994); Joseph Eaton, CARD-CARRYING AMERICANS: PRIVACY, SECURITY, AND THE NATIONAL ID CARD DEBATE 94-97 (1986); *but see* Enrico Cantoni & Vincent Pons, *Strict ID Laws Don't Stop Voters: Evidence from a U.S. Nationwide Panel, 2008–2018*, 136 Q.J. ECON. 2615, 2615 (2021) (study showing that voter ID laws in 11 states had no effect on preventing voter fraud nor on dampening registration or turnout).

[14] Magdalena Krajewska, DOCUMENTING AMERICANS: A POLITICAL HISTORY OF NATIONAL ID CARD PROPOSALS IN THE UNITED STATES 3 (2017) ("Only three OECD countries, the United States, Ireland, and New Zealand, never had national ID cards, not even during wartime. There is no major country outside the OECD that also lacks a national ID card.").

[15] *See* Berman, *supra* note 12.

raised against the creation of a national ID in the U.S., but they can broadly be categorized into three buckets: fear of surveillance, fear of exploitation, and fear of exclusion.[16]

A. Fear of Surveillance

One of the most often cited reasons for opposing the use of national IDs is the potential risk of the government using this powerful tool as a means of surveillance. The use of national identifiers expands the police power of a country's government. Many countries have used national IDs to fight crime, corruption, and fraud; other countries have used them to profile race, ethnicity, political views, and religion.[17] A national ID database in the hands of the government therefore can mean exciting potential benefits)as well as terrifying harms—for example, the government could effectively compile lists of political dissenters using the same data-matching capability that allows it to effectively detect tax evasion. Worried that national ID would amplify the government's surveillance capability, libertarians on the right often decry its threats to individual privacy and liberty, while civil rights advocates on the left frequently predict that IDs would inevitably lead to the discrimination and harassment of minorities.[18] Governmental anti-terrorism efforts focused on mandatory ID or tracking,[19] and Edward Snowden's revelations on American intelligence operations' surveillance practices [20] have bolstered fears of government surveillance supplemented by a national ID system. Any proposal

---

[16] Adapted from Privacy International's list of potential harms of digital national ID. *See* PRIV. INT'L, DIGITAL NATIONAL ID SYSTEMS: WAYS, SHAPES AND FORMS (Oct. 26, 2021), https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms [https://perma.cc/C9EQ-HCAD].

[17] *Mandatory National IDs and Biometric Databases*, ELEC. FRONTIER FOUND. [EFF], https://www.eff.org/issues/national-ids [https://perma.cc/U2DL-RKYK] (last visited Apr. 1, 2022); *see also* Neda Matar, Comment, *Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy*, 17 EMORY INT'L L. REV. 287, 296 (2003).

[18] Jim Harper, *The New National ID Systems*, CATO INSTITUTE (Jan. 30, 2018), https://www.cato.org/policy-analysis/new-national-id-systems [https://perma.cc/9UZA-NJ56]; AM. CIV. LIBERTIES UNION [ACLU], 5 PROBLEMS WITH NATIONAL ID CARDS, https://www.aclu.org/other/5-problems-national-id-cards [https://perma.cc/4Y8R-YSVL] (last visited Apr. 1, 2022); EFF, *supra* note 17.

[19] PRIVACY INT'L, *supra* note 16.

[20] LAWFARE BLOG, SNOWDEN REVELATIONS, https://www.lawfareblog.com/snowden-revelations [https://perma.cc/5TPX-52ZJ] (last visited Apr. 1, 2022); Glen Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (Jun. 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/47FJ-G8LM].

to establish a national ID system in the U.S. must include provisions that will sufficiently assuage those fears.[21]

B. Fear of Exploitation

The fear of exploitation similarly involves the abuse of the unique identifier, a key feature of any national ID system. As an individual uses the same unique identifier—often a string of numbers—to conduct everyday transactions, it becomes exceedingly easy for an unregulated actor to aggregate mountains of information about the individual into a virtual or real dossier. Depending on the context and use of the dossier, this act of aggregation may not be in and of itself alarming. Government agencies could, with the American people's knowledge and consent, match databases that were previously separate using unique identifiers to deliver benefits more efficiently.[22] However, government agencies could also use unique identifiers in ways that can harm privacy and civil liberties.[23]

In addition to the public sector, exploitation can also happen in the private sector. Private companies have been compiling information on millions of Americans even without a national ID system by maintaining their own list of profiles.[24] Once a national ID is established, a unique identifier backed by the government would be of considerable interest to private actors that depend on reliable authentication and data-matching as part of their daily operations. A secure and reliable national ID system would allow companies to improve user experience, conduct accurate attribute verification (e.g., checking someone's age for sale of regulated products), and lower the risk of online fraud —advantages that are especially appealing to companies in banking, financial services, retail, and travel sectors.[25] While such uses surely

---

[21] *See* discussion of such provisions Part IV, *infra*.

[22] For example, the Internal Revenue Service could data match with the Department of Education to automatically apply tuition-related tax deductions and determine eligibility for state-sponsored financial aid.

[23] For example, border authorities could populate no-fly lists based on data from unrelated agencies.

[24] Large digital platform companies such as Google and Meta (formerly Facebook) even keep track of non-users on their databases. *See, e.g.*, Anthony Caruana, *What You Need To Know About Your Google Shadow Profile*, LIFEHACKER (Mar. 14, 2019, 11:45 AM), https://www.lifehacker.com.au/2019/03/what-you-need-to-know-about-your-google-shadow-profile/ [https://perma.cc/4EUX-AEPB]; Russell Brandom, *Shadow profiles are the biggest flaw in Facebook's privacy defense*, THE VERGE (Apr. 11, 2018, 3:53 PM), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy [https://perma.cc/2UYM-CXF4].

[25] Frederic Ho, *How National Digital IDs Benefit Both Citizens And Businesses*, FORBES (May 3, 2021), https://www.forbes.com/sites/jumio/2021/05/03/how-national-digital-ids-benefit-both-citizens-and-businesses/ [https://perma.cc/862J-UPU4].

benefit consumers, they can also substantially harm data privacy protections by providing private data collectors and brokers with a convenient tool to gather information on any individual to sell on a hungry market. Companies like Google or Meta (formerly Facebook) could combine their existing stockpiles of online user data with the national ID system to vastly extend the reach of their personalized advertising.[26] A national ID system implemented without regulations in place to prevent such practices would predictably lead to open commercial exploitation—an eventuality that we have already seen with the Social Security Number.[27]

Finally, exploitation can happen in the form of increased risk of identity theft and the introduction of false information in the system.[28] A centralized location of the information underlying the national ID system would enable large numbers of entities to access data for a wide range of purposes, but it would also make the system more vulnerable to false information being injected due to illicit modification or data input error. A large central database of identities would also likely be a common target of identity theft, such as those resulting from the reported data leaks in India's Aadhar database and the voter registration database of the Philippines.[29]

C. Fear of Exclusion

Over-dependence on a national ID system poses risks to those excluded by that system. In other words, as more people rely on national ID to access public benefits and conduct business, it becomes more discriminatory and costly to those in the population who are unable to verify

---

[26] Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have On You*, SECURITY.ORG (Mar. 23, 2022), https://www.security.org/resources/data-tech-companies-have/ [https://perma.cc/LKG3-SCLB]; Andrew Quodling, *Shadow profiles - Facebook knows about you, even if you're not on Facebook*, THE CONVERSATION (Apr. 13, 2018), https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804 [https://perma.cc/U8E2-P3QP].

[27] *See* Section II.D, *infra*.

[28] EFF, *supra* note 17; A. Michael Froomkin, *The Uneasy Case for National ID Cards as a Means to Enhance Privacy* 305 (2008); SECURING PRIVACY IN THE INTERNET AGE (A. Chander, L. Gelman, M.J. Radin, eds 2008), https://ssrn.com/abstract=2719008 [https://perma.cc/DT4V-AX6T]; PRIV. INT'L, *Understanding Identity Systems Part 3: The Risks of ID* (Jan. 31, 2019), https://www.privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id [https://perma.cc/YC2M-8YVM].

[29] Zack Whittaker, *A new data leak hits Aadhaar, India's national ID database*, ZDNET (Mar. 23, 2018), https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/ [https://perma.cc/B6GQ-6B96]; Leisha Chi, *Philippines elections hack 'leaks voter data'*, BBC (Apr. 11, 2016), https://www.bbc.com/news/technology-36013713 [https://perma.cc/ES8P-WWBG].

themselves and enroll in the system.[30] Exclusion can occur inadvertently, such as by logistical or technical failures. This results in groups of people being left without IDs, even as the government increases ID restrictions on access to critically important social programs and benefits.[31] National ID systems based on biometrics can also end up excluding people who are physically unable to provide the necessary biometrics—manual laborers, the elderly whose fingerprints fade over time, or people with missing limbs.[32]

Exclusion can also happen by design. Governments can target a group of people to be identified on their IDs (e.g., tagged with a certain word, or an identity number in a different range from the rest of the population) to be set apart and treated differently.[33] Examples of such practices include Myanmar's forced issuance of identity documents to the Rohingya minority, and Kenya issuing people of Somali descent a different colored identity document to make them more easily identified by law enforcement.[34] Besides overt discriminatory policies, the government could also exclude people as a means of regulation or punishment, especially if people are dependent on the national ID. A ubiquitous national ID that is used for everyday purchases, age verification, travel, and transportation could be leveraged as a chokepoint where sanctions could be applied.[35]

Finally, it goes without saying that the three fears discussed above do not fully cover the range of concerns voiced by critics of national ID systems. For example, these fears assume a national ID system with complete and accurate data. This is a shaky assumption in practice. For example, identification via social security number can lead to verification errors quite frequently.[36] The possibility of inaccurate information being introduced to the

---

[30] PRIV. INT'L, *supra* note 16.

[31] PRIV. INT'L, *Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations* (Mar. 29, 2021), https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible [https://perma.cc/UCD6-MWF8].

[32] *Id.* A particularly tragic story in India involved people starving to death after being denied food rations due to their fingerprints not being recognized. *See* Nikhil Dey & Aruna Roy, *How Chunni Bai's death exposes the lie about Aadhaar*, THE TIMES OF INDIA (Sept. 30, 2018), https://timesofindia.indiatimes.com/home/sunday-times/all-that-matters/how-chunni-bais-death-exposes-the-lie-about-aadhaar/articleshow/66009239.cms [https://perma.cc/X8TE-NTFV].

[33] PRIVACY INT'L, *Exclusion and identity: life without ID* (Dec. 14, 2018), https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id [https://perma.cc/6BA4-3PAA].

[34] *Id.*

[35] Froomkin, *supra* note 28, at 307.

[36] *See* Bob Sullivan, *Odds someone else has your SSN? One in 7*, NBC NEWS (Dec. 3, 2010, 9:00 AM), https://www.nbcnews.com/technolog/odds-someone-else-has-your-ssn-one-7-6c10406347 [https://perma.cc/DA5Z-MGKE].

national ID system also compounds the intensity of critics' fears: A false positive match could subject the wrong person to law enforcement scrutiny or exclude someone who does meet eligibility requirements from receiving government benefits.

D. A Case of Failure: The Social Security Number

The story of the Social Security Number (SSN) illustrates how all three of these fears— surveillance, exploitation, and exclusion—play out in what is considered the closest thing the U.S. currently has to a government-run national ID scheme.

When the SSN was created in 1936, its original purpose was to act as an account number to facilitate the administration of the Social Security system.[37] The number was intended to be used to track a worker's lifetime earnings so that the Social Security Administration could determine their retirement benefits.[38] However, noting the trend of the SSN's wider adoption for purposes unrelated to social security, a Social Security Administration task force in 1971 warned against promoting the use of the SSN as an identifier, while a Department of Health, Education and Welfare report warned that a national identifier would "enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated systems." [39] Citing similar privacy concerns, both the Nixon and Carter Administrations rejected SSNs as a national uniform identifier.[40] Even in the wake of the September 11 attacks

---

[37] ELEC. PRIV. INFO. CTR. [EPIC], *National ID and the REAL ID Act*, https://archive.epic.org/privacy/id_cards/ (last visited Apr. 1, 2022) [https://perma.cc/WJX2-5L2N].

[38] Adrianne Jeffries, *Identity crisis: how Social Security numbers became our insecure national ID*, THE VERGE (Sept. 26, 2012, 12:00 PM), https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic [https://perma.cc/W55P-C8RA].

[39] SOC. SEC., *Social Security Number Chronology*, https://www.ssa.gov/history/ssn/ssnchron.html (last visited Apr. 1, 2022) [https://perma.cc/4UWG-6ZRX]; DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS § VIII (Jun. 30, 1973), https://aspe.hhs.gov/reports/records-computers-rights-citizens [https://perma.cc/QC8N-MKEN] ("What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems.").

[40] *Coalition Letter to Secretary Mineta Urging Opposition to a Backdoor National ID System*, ACLU (last visited May 16, 2022), https://www.aclu.org/letter/coalition-letter-secretary-mineta-urging-opposition-backdoor-national-id-system [https://perma.cc/WC3N-BL67].

when public support for a national ID reached 70 percent,[41] Congress included language in the enabling legislation for the Department of Homeland Security that clarified that the agency did not have the authority to create a national ID system.[42] In 2005, a bipartisan commission co-chaired by former President Jimmy Carter endorsed a federal voter ID requirement, with SSNs seen as the "most feasible option for a federal unique identifier."[43] The commission's recommendations were swiftly denounced by Democrats in Congress, including then-Senator Barack Obama and Representative John Lewis.[44]

Despite such consistent opposition to the SSN becoming a national ID, it has become one by default, perhaps because other forms of identification are even less suitable: Not everyone owns a passport, and birth certificates are not standardized across states.[45] The SSN today is requested as an identifying number by private companies and government agencies alike; an SSN is typically required to open a bank account, to apply for a federal loan, to receive government benefits for unemployment and Medicare, or to file taxes.[46] If anything, the ubiquitous use of the SSN as an identifier has demonstrated the market demand for a unique identifier as a means of identity verification and authentication.

The story of the SSN is the story of exploitation and exclusion. SSNs have been at the center of major security and identity theft events, including the infamous hack of the U.S. Office of Personnel Management, inwhere 21.5 million SSNs were stolen.[47] Indeed, SSNs have become available "through data resellers, security breaches at various companies and government agencies, unsuspecting customer service representatives, and even public records."[48] And though the Privacy Act forbids agencies from denying government service or benefit for failure to provide one's SSN (unless federal law specifically requires it),[49] this protection does not extend to the private

[41] Berman, *supra* note 12.
[42] EPIC, *supra* note 37; Homeland Security Act § 1514, 6 U.S.C. § 101 (2002).
[43] COMM'N ON FED. ELECTION REFORM, BUILDING CONFIDENCE IN U.S. ELECTIONS 13 (Sept. 2005), https://www.eac.gov/sites/default/files/eac_assets/1/6/Exhibit%20M.PDF [https://perma.cc/RJ3P-3GUG].
[44] Berman, *supra* note 12.
[45] Jeffries, *supra* note 38.
[46] Amy Fontinelle, *The Purpose of Having a Social Security Number*, INVESTOPEDIA (Mar. 6, 2023), https://www.investopedia.com/articles/personal-finance/050615/purpose-having-social-security-number.asp [https://perma.cc/MT3Z-993R].
[47] Brian Naylor, *OPM: 21.5 Million Social Security Numbers Stolen From Government Computers*, NPR (July 9, 2015, 9:40 PM), https://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers [https://perma.cc/4P4V-KMPU].
[48] Jeffries, *supra* note 38 ("SSNs can be bought in bulk for $1 each on private online forums, and a specific person's SSN can reportedly be had for as little as $3.80.").
[49] 5 U.S.C. § 552a note (Disclosure of Social Security Number); 5 U.S.C. § 7(a)(1).

sector. Companies can choose not to do business with someone if they refuse to provide their SSN, and no federal law currently exists that prevents businesses from requesting SSNs from consumers.[50] Based on the history of the SSN alone, it is not hard to see why Americans would hesitate to support any attempt to create a new national ID system.

E. A Case of Potential Failure: REAL ID

Around the same time former President Carter's bipartisan commission on election reform was established Congress passed the REAL ID Act of 2005.[51] Drafted and passed during the height of the global war on terror, the Act's stated purpose notably included the interest of "prevent[ing] terrorists from abusing the asylum laws of the United States."[52] The author of the bill further emphasized the counterterrorism purpose underlying the bill, stating that REAL ID will "hamper the ability of terrorist and criminal aliens to move freely throughout our society."[53] Though the REAL ID Act was originally stalled in the Senate, the author of the bill attached it as a rider on a military spending bill that dealt with emergency appropriations for the Iraq War and tsunami relief funding.[54] The statute calls for the creation of national standards for state-issued driver's licenses and ID cards, such that IDs must meet those standards when used for accessing certain federal facilities and—most relevant to the average American—for air travel.[55] The Department of Homeland Security denies that REAL ID effectively creates national ID database because the program leaves the issuance of cards and the maintenance of databases to the States.[56] As of this writing, all states and

[50] The State of New York recently passed a law that prohibits companies from refusing service to customers without a social security number. N.Y. GEN. BUS. LAW § 399-ddd. ("Confidentiality of social security account number").
[51] REAL ID Act, Pub. L. No. 109-13, 119 Stat. 302 (2005).
[52] REAL ID Act, BALLOTPEDIA, https://ballotpedia.org/REAL_ID_Act_of_2005 (last visited May 11, 2022).
[53] Declan McCullagh, *FAQ: How Real ID will affect you*, CNET (May 6, 2005), https://www.cnet.com/tech/tech-industry/faq-how-real-id-will-affect-you/ [https://perma.cc/8NE2-TS4P].
[54] BALLOTPEDIA, *supra* note 52 *see also* REAL ID Act, WIKIPEDIA, https://en.wikipedia.org/wiki/Real_ID_Act [https://perma.cc/EZH7-JTJX] (last visited May 11, 2022).
[55] *About REAL ID*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/real-id/about-real-id [https://perma.cc/RXK5-895Z] (last visited May 11, 2022).
[56] REAL ID Frequently Asked Questions, DEP'T OF HOMELAND SEC., https://www.dhs.gov/real-id/real-id-faqs [https://perma.cc/X22W-Z467] (last visited May 11, 2022).

territories have been certified as REAL ID compliant except American Samoa, which is under review.[57]

Setting aside the argument that REAL ID will probably fail to prevent terrorism,[58] the program could also be considered a failure as a national ID for public benefits. Because it was designed as a tool for identifying and removing U.S. people suspected of terrorism-related activities from the U.S.,[59] REAL ID will inevitably serve those interests rather than the public interest of access to government services and benefits. REAL ID-compliant driver's licenses may provide safe commercial flights; they will not provide secure personal healthcare records or efficient tax benefit eligibility determination. While the SSN is a failure story due to a lack of adequate accompanying rules preventing issues such as function creep,[60] REAL ID is doomed to fail as a national ID for public purpose because it was born out of the government's fear and distrust of the public, instead of its desire to serve the public.

III. HOPES AND HIGHLIGHTS

Despite these legitimate fears and troubling failures with national ID, technological developments in the last decade offer reasons for the United States to be optimistic of a secure and reliable national ID regime. Examples abound of cryptographic techniques, ranging from the largely theoretical to those already incorporated into secure transactions, that could enable a secure national ID system. Advances in cryptography offer key ingredients for identity verification systems that have been successfully implemented both here and abroad.

F. Technological Advances

A technology that captured the public's attention and swept headlines in recent years could be a key piece of the national ID puzzle. Distributed ledger technology, especially as implemented in blockchain, has already been

---

[57] REAL ID, DEP'T OF HOMELAND SEC., https://www.dhs.gov/real-id [https://perma.cc/X22W-Z467] (last visited May 11, 2022).

[58] *See* ACLU, *supra* note 18 (National ID "would not have thwarted the September 11 hijackers, for example, many of whom reportedly had identification documents on them, and were in the country legally. Terrorists and criminals will continue to be able to obtain—by legal and illegal means—the documents needed to get a government ID, such as birth certificates.").

[59] The bill's author, Rep. James Sensenbrenner, noted that the REAL ID Act will "hamper the ability of terrorist and criminal aliens to move freely throughout society . . .". Ashley Feinberg, *What is Real ID?* GIZMODO (Jan. 20, 2014, 1:27 PM), https://gizmodo.com/what-is-real-id-1505105796 [https://perma.cc/M2NU-MZZL].

[60] *See* Section IV, *infra*, for further discussion on function creep.

heralded as a potentially transformational technology for government services.[61] Generally speaking, a blockchain is a "distributed database that is stored on various nodes (the computers that store a copy of the database) and maintained by a consensus algorithm."[62] Blockchains are used to log transactions in an append-only manner, meaning that information can always be added but never removed. The cryptographic hash-chaining process of the blockchain renders the log tamper-evident, promoting transparency and accountability by design.[63] As such, the guarantee of integrity for transaction records and data to a mathematical certainty makes blockchain valuable for society and governance.[64] So far, blockchain technology has been used to: create smart contracts, reducing transaction time by 90% in Sweden; register land ownership and real estate transactions in the country of Georgia; administer pensions in the Netherlands; and verify academic credentials for employment purposes in Malta.[65] Similarly, blockchain technology could substantially boost the transparency and reliability of a national ID system, which would in turn foster public trust.[66]

While still largely theoretical and less well-known than blockchain, a mathematical method called Zero-Knowledge Proof (ZKP) may also influence national ID design. ZKP allows one party to verify information about another

---

[61] Victoria Lemieux & Cem Dener, *Blockchain technology has the potential to transform government, but first we need to build trust*, WORLD BANK BLOGS (Dec. 2, 2021), https://blogs.worldbank.org/governance/blockchain-technology-has-potential-transform-government-first-we-need-build-trust [https://perma.cc/X2MF-A56T]; *see generally* IBM, WHAT IS BLOCKCHAIN TECHNOLOGY?, https://www.ibm.com/topics/what-is-blockchain (last visited Apr. 4, 2022) [https://perma.cc/XH8V-H72E].

[62] EUROPEAN COMMISSION, STUDY ON BLOCKCHAINS: LEGAL, GOVERNANCE AND INTEROPERABILITY ASPECTS 26 (Feb. 2020), https://data.europa.eu/doi/10.2759/4240 [https://perma.cc/X3RP-MCB8].

[63] *Id.* at 27.

[64] Helen Eenmaa, *Sovereignty and Autonomy Via Mathematics*, 4 STAN. J. BLOCKCHAIN L. & POL'Y 79, 97 (2021).

[65] *See* Ameep Pandey, *How governments can harness the potential of blockchain*, MCKINSEY DIGIT. (Nov. 6, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/how-governments-can-harness-the-potential-of-blockchain [https://perma.cc/3F94-YL4D]. *But see* Mike Orcutt, *Once hailed as unhackable, blockchains are now getting hacked*, MIT TECH. REV. (Feb. 19, 2019), https://www.technologyreview .com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ [https://perma.cc/Q6NQ-EU59] (describing various potential security vulnerabilities in blockchain technologies).

[66] Notably, the system does not *need* users' trust—the mathematical certainty of the system allows it to guarantee data integrity and reliability, with or without trust among participants. *See* Eenmaa, *supra* note 64, at 96.

party without revealing anything about the content of the information.[67] Possible applications of the ZKP include checking whether an account has enough money to complete a transaction without knowing the balance itself, confirming a password's validity without needing to directly process it, or even verifying nuclear weapons without revealing classified information in support of disarmament efforts.[68] Given the powerful advantages ZKP brings to transactions involving secure and confidential authentication of data, researchers are already looking into how it can be used for ID mechanisms.[69] A national ID system that uses zero-knowledge protocols could assuage much of the fears associated with surveillance and exploitation; even though the government manages national IDs, it would not be able to learn anything about the underlying data without consent by the data subjects.

But even if some of the theories and methods such as ZKP do not turn out to be as promising in practice, or if they are not mature enough to support nationwide deployment, there are already secure infrastructures used in national ID systems around the world that the U.S. can emulate and improve upon. The most prominent example of a secure, transparent, and reliable national ID scheme is Estonia's e-ID system.

G. Build for the People: Estonia's e-ID

pretium. Praised as the world's most digitally advanced society, Estonia started building the foundations for its national digital ID and e-government infrastructure soon after its independence from Russia in 1991.[70] Noting that the passports it started issuing in 1992 would expire in 10 years, the Estonian government decided to use the expiration as an opportunity to

---

[67] Lily Hay Newman, *Hacker Lexicon: What Are Zero-Knowledge Proofs?*, WIRED (Sept. 14, 2019, 7:00 AM), https://www.wired.com/story/zero-knowledge-proofs/ [https://perma.cc/5TUJ-PRPT].

[68] *Id.*; Chris Sadler, *Verification Without Information: The Promise of Zero-Knowledge Proofs*, NEW AM. (Apr. 2, 2020), https://www.newamerica.org/oti/blog/verification-without-information-promise-zero-knowledge-proofs/ [https://perma.cc/97M3-F2PH].

[69] *Id.*; Pamela Dingle, *Advancing Privacy with Zero-Knowledge Proof Credentials*, MICROSOFT TECH CMTY. (Jul. 22, 2020, 9:00 AM), https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554 [https://perma.cc/V5R9-XQLJ]; Nuttawut Kongsuwan, *Minimal Disclosure of Identity with Zero-Knowledge Proof and CL-Signature*, FINEMA (Apr. 6, 2020), https://medium.com/finema/minimal-disclosure-of-identity-with-zero-knowledge-proof-and-cl-signature-517ed2a61307 [https://perma.cc/6G3N-YMUB].

[70] Ben Hammersley, *Concerned about Brexit? Why not become an e-resident of Estonia*, WIRED (Mar. 27, 2017), https://www.wired.co.uk/article/estonia-e-resident [https://perma.cc/ET82-SKLQ]; Matt Reynolds, *Welcome to E-stonia, the world's most digitally advanced society*, WIRED (Oct. 20, 2016), https://www.wired.co.uk/article/digital-estonia [https://perma.cc/B9GQ-7CN7].

introduce a new ID card in 2002 that would provide Estonian residents with the ability to sign agreements digitally.[71] Coupled with the government offering free Wi-Fi connectivity in most populated areas in the same year and continuing to invest in Internet infrastructure, Estonia's e-ID quickly became the population's main means of securely accessing private and public websites and conducting business online.[72] The e-ID is available as a physical smart card, as well as digital and mobile IDs, and allows Estonian citizens to access 99 percent of public services online 24 hours a day—the only thing people cannot do online is get married and get divorced.[73]

The ID system itself operates on the basis of a public key infrastructure, which is a combination of policies, procedures, and technology supporting the management of digital certificates and public key encryption to ensure secure communication and authentication.[74] After experiencing a major cyberattack by Russia in 2007, Estonia incorporated a homegrown blockchain technology called Keyless Signature Infrastructure (KSI) Blockchain to protect the integrity of government networks and data while "guaranteeing 100% record privacy."[75] Enabling continuous integrity monitoring for all kinds of digital assets and data objects, the KSI blockchain is used to back the Estonian state registries for healthcare, property, business, and succession, along with the digital court system and the official state announcements system.[76] Along with integrity and transparency afforded by the KSI blockchain, Estonia also gives e-ID users control over their data through the data tracker, which allows users to log into a state portal and "review the full list of queries concerning their personal information."[77] The

---

[71] Arnis Parsovs, *Estonian Electronic Identity Card and its Security Challenges* 17 (Mar. 3, 2021) (Ph.D. dissertation, University of Tartu), https://perma.cc/V565-X77R.

[72] Hammersley, *supra* note 70.

[73] E-ESTONIA, E-GOVERNANCE: GOVERNMENT CLOUD, https://e-estonia.com/solutions/e-governance/government-cloud/ [https://perma.cc/MHS9-GAEY] (last visited Apr. 2, 2022); Rob Pegorado, *This country moved its government online. Here's why that wouldn't fly in the U.S.*, FAST CO. (Sept. 10, 2021), https://www.fastcompany.com/90671437/estonia-digital-citizenry-evoting [https://perma.cc/44SR-PYJX].

[74] EUR. UNION AGENCY FOR CYBERSECURITY [ENISA], GLOSSARY: PUBLIC KEY INFRASTRUCTURE (PKI), https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/publicpublic-key-infrastructure-pki [https://perma.cc/LU46-GCFR] (last visited Apr. 2, 2022).

[75] *See KSI Blockchain in Estonia*, E-ESTONIA, https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf [https://perma.cc/TE7G-MNVU] (last visited Apr. 4, 2022); Pegorado, *supra* note 73.

[76] Estonia also plans to bring its data embassies, smart grid, personalized medicine, cyber-defense, and electronic taxation on KSI blockchain in the future. *See* E-ESTONIA, *supra* note 73.

[77] *Data tracker - tool that builds trust in institutions*, E-ESTONIA (Sept. 18, 2019), https://e-estonia.com/data-tracker-build-citizen-trust [https://perma.cc/8KFY-5ZMA].

data tracker tool thus allows citizens and residents to keep an eye on how their personal data is being accessed and used by major government agencies.[78] Reports of security incidents or abuse of Estonia's e-ID system are rare: If there ever are any issues, they are quickly rectified thanks to the accountability and transparency measures in place.[79]

The e-ID system most recently proved its value to the Estonian people when its e-Health record system facilitated accurate contact tracing and produced daily statistics for public health officials during the COVID-19 pandemic, contributing to the country faring better than many of its European neighbors at the start of the pandemic.[80] Even in non-pandemic times, the e-Health Record allows Estonians to control their health data: They can see whenever someone accessed part of their health record, and only physicians and people that they specifically authorize can access their data.[81] Health records from different hospitals and clinics are aggregated in a central repository, viewable in a standard format by patients and physicians. The KSI Blockchain technology ensures the accuracy and integrity of medical information and access logs.[82]

Estonia's e-ID system effectively responds to each of the fears discussed in Section II. Fears of surveillance and exploitation are overcome through transparency measures, imposed by technical design (e.g., the KSI Blockchain keeps an immutable ledger of activity) and by data protection rules under the EU's General Data Protection Regulation.[83] Rather than fearing exclusion, Estonians built the e-ID system for inclusion: All Estonians, regardless of race, gender, or socioeconomic status, can obtain a digital ID and reap its benefits. Even non-Estonians can become e-residents of Estonia to

---

[78] *Id.*

[79] *See ID systems analysed: e-Estonia*, PRIV INT'L (Jan. 12, 2022), https://privacyinternational.org/case-study/4737/id-systems-analysed-e-estonia [https://perma.cc/9DJY-E7MJ]. For a more in-depth discussion of security incidents involving e-ID, *see* Parsovs, *supra* note 71.

[80] Morgan Meaker, *How Estonia used its digital state to beat back coronavirus*, WIRED (June 19, 2020), https://www.wired.co.uk/article/estonia-coronavirus [https://perma.cc/8F8X-QVLV].

[81] *See* DIGIEXPO E-ESTONIA, NATIONAL ELECTRONIC HEALTH RECORD, https://digiexpo.e-estonia.com/Solutions/helmes-national-electronic-health-record/ [https://perma.cc/UF88-HWCZ] (last visited Apr. 5, 2022).

[82] *Id.*

[83] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 2, 2016 O.J. L 119/1 [hereinafter GDPR].

access various public services and the EU economy, allowing them to trade goods and services in the world's largest single market.[84]

H. A Case for Hope: PIV Cards in the U.S. Government

We can be optimistic about a publicly owned, secure, and reliable national ID in the U.S. because key technologies underlying Estonia's e-ID system are already being used here, albeit in a more limited scale. For example, the Department of Defense has contracted with the key supplier of Estonia's KSI Blockchain software and services to ensure the security of its supply chains.[85] In addition, a small but significant subset of the American population is already using an ID system built on public key infrastructure: 5 million federal employees and contractors use Personal Identity Verification (PIV) cards every day to log onto their government-issued computers, access and manage secure documents, as well as provide and authenticate digital signatures.[86] While these examples do not automatically suggest that these use cases can be scaled nationwide for every person in the country, they demonstrate at the very least that the U.S. clearly has the capacity to implement a secure and reliable ID system like Estonia's. The question is, should it establish such a national ID system, and if so, what would implementation entail?

IV. IT CAN (AND IT SHOULD) HAPPEN HERE

The U.S. should create a national ID for public purpose as a much-needed substitute for the privately-owned, fragmented system we have today which poses significant surveillance and exploitation risks to the American people. Setting up the system will not be easy and numerous hurdles need to be overcome to achieve successful implementation. To minimize risks of surveillance, exploitation, and exclusion, the U.S. should establish data

---

[84] *See* Hannah Brown, *is e-residency for me*? ESTONIA E-RESIDENCY (Mar. 19, 2021), https://www.e-resident.gov.ee/blog/posts/is-e-residency-for-me [https://perma.cc/V785-7DG2]; EU position in world trade, EUR. COMM'N, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/eu-position-world-trade_en [https://perma.cc/FX86-U6JM] (last visited May 17, 2022); *see also* Hammersley, *supra* note 70.

[85] E-ESTONIA, *supra* note 73; *Adding Blockchain Capabilities for DoD and IC Customers*, NAT'L CTR. FOR MFG. SCIENCES (May 4, 2018), https://www.ncms.org/adding-blockchain-capabilities-for-dod-and-ic-customers/ [https://perma.cc/8X9R-T9Z7].

[86] NAT'L INST. STANDARDS & TECH., *Personal Identity Verification (PIV)*, https://www.nist.gov/topics/identity-access-management/personal-identity-verification-piv [https://perma.cc/X7CC-V8UU] (last visited Apr. 4, 2022); DIGITALVA, *Personal Identity Verification (PIV)*, https://www.oit.va.gov/programs/piv/index.cfm [https://perma.cc/RXU7-5HVV] (last visited Apr. 4, 2022).

protection rules that protect against function creep and give individuals control over their own data.

I. An Urgent Need for a Public Alternative

The most pressing reason for the U.S. to implement a national ID is that we already have one; the problem is that it is owned by a multitude of powerful private companies that have assembled comprehensive profiles on every person in the country. This de facto national ID is therefore designed to extract from the people, rather than to serve them. A former Secretary of Homeland Security reportedly stated that "[w]e do have a national ID. It's operated by giant tech companies, where every place you are, everything you do, everything you search for is recorded in some fashion and integrated as a matter of managing your data."[87]

In addition, private data brokers have acted as "the middlemen of surveillance capitalism" for years, aggregating information about individuals from a hodgepodge of data sources and selling the records to any interested buyer, including law enforcement agencies.[88] Law enforcement agencies in particular have been reported to purchase data on millions of consumers from third-party data brokers that maintain massive private databases.[89] Though government would otherwise be restricted from directly collecting information on individuals without proper authorizations and procedures, agencies are largely able to bypass those restrictions by dealing with data intermediaries. As a result, we are left with a distribution of databases owned by private actors that are endlessly gathering and profiting from data on American consumers.[90]

---

[87] Berman, *supra* note 12.

[88] Drew Harwell, *Utility giants agree to no longer allow sensitive records to be shared with ICE*, WASH. POST (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/ [https://perma.cc/78CF-J8LY]; Justin Sherman, *Data Brokers Are a Threat to Democracy*, WIRED (Apr. 13, 2021), https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/ [https://perma.cc/JX3V-2B3L]; 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 (2003), https://scholarship.law.unc.edu/ncilj/vol29/iss4/1.

[89] Sharon Bradford Franklin et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/ [https://perma.cc/XD57-ZQPN]; *Data Brokers*, EPIC, https://epic.org/issues/consumer-privacy/data-brokers/ (last visited May 17, 2022) [https://perma.cc/M379-3PQP].

[90] Vigderman and Turner, *supra* note 26; Angela Moscaritolo, *What Does Big Tech Know About You? Basically Everything*, PCMAG (Jan. 18, 2022),

Advertiser identifiers ("ad IDs"), the unique IDs used by digital advertising firms to track individual consumers and their behavior, enable the data brokers to sell this data to federal and local law enforcement agencies.[91] This in turn allows government agencies like the Immigration and Customs Enforcement (ICE) to engage in surveillance while escaping public scrutiny.[92]

Because the private companies each own separate databases, individuals end up absorbing the cost of managing their profiles in each system (e.g., remembering different passwords for financial institutions, or transferring health records from one hospital system to another) and bearing the burden of keeping track of multiple avenues through which security breaches may occur.[93] The privately-owned national ID we currently have is the worst of all worlds—the ID's usefulness is undermined by its fragmentation and the high transaction costs for each data matching operation; information that populates the databases are mostly collected without the data subject's knowledge or consent; and the ID does not deliver public benefits of any kind.

This status quo is unacceptable. The U.S. urgently needs a secure, accountable, and inclusive national ID system that is governed by strong data protection rules. Having a uniform national ID system managed by the government and held accountable to the people is strongly preferable to the de facto ID system owned by a patchwork of largely unregulated private actors acting in their self-interest.

J. Implementation Challenges

https://www.pcmag.com/news/what-does-big-tech-know-about-you-basically-everything [https://perma.cc/274Y-YTLG].

[91] *See* Garance Burke and Jason Dearen, *Tech tool offers police 'mass surveillance on a budget,'* THE ASSOCIATED PRESS (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef [https://perma.cc/9Z58-74TV]; Will Greenberg, *How Ad Tech Became Cop Spy Tech*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/how-ad-tech-became-cop-spy-tech [https://perma.cc/6BZP-6RS7].

[92] *American Dragnet: Data-Driven Deportation in the 21st Century*, GEO. L. CTR. ON PRIV. & TECH. (May 10, 2022), https://www.americandragnet.org/ [https://perma.cc/A7WC-ERDA] ("By reaching into the digital records of state and local governments and buying databases with billions of data points from private companies, ICE has created a surveillance infrastructure that enables it to pull detailed dossiers on nearly anyone, seemingly at any time.").

[93] Having to maintain multiple accounts can lead to an expanded "attack surface" potentially vulnerable to security breach. *See* Lily Hay Newman, *Hacker Lexicon: What Is an Attack Surface*?, WIRED (Mar. 12, 2017, 8:00 AM), https://www.wired.com/2017/03/hacker-lexicon-attack-surface/ [https://perma.cc/F6T8-HMNP].

We must of course acknowledge that establishing an Estonia-like e-ID system in the United States will come with significant challenges. Unlike Estonia's experience with introducing its e-ID when its first passports began to expire, the U.S. does not have a natural timepoint for migration to the new ID. The U.S. also has a vast and complex legacy infrastructure to reckon with, such as the REAL ID driver's license standards, databases, and card readers. Furthermore, the U.S. has over 200 times the landmass and nearly 250 times the population of Estonia.[94] The adoption of a new national ID will certainly take more time and resources to complete; distributing the new IDs to the American people poses its own challenges.

At the same time, the U.S. should reckon with existing distributional inequities across socioeconomic levels and in rural communities. One serious inequity issue relevant to national ID is the digital divide: a national ID that offers expanded access to government services through digital technologies will be of little use to those who have limited access to those technologies. Students in lower-income families and Black teens were more likely to face obstacles in remote learning contexts during the COVID-19 pandemic due to a lack of access to a computer or to a reliable Wi-Fi connection.[95] Despite positive trends in recent years, rural Americans are still less likely to have broadband access at home and have lower levels of technology ownership compared to Americans in urban and suburban areas.[96] Americans with disabilities also report lower technology ownership compared to those without disabilities.[97] For the new national ID to be accessible to the very people who will benefit from it most, the U.S. must close its digital divide.

Related to the digital divide is the hobbled state of the U.S. Postal Service (USPS). Relatively poor access to the Internet often means that rural Americans rely more heavily on mail. Because private businesses like FedEx or UPS do not deliver to remote rural areas, Americans who live in those areas

---

[94] *Country comparison Estonia vs United States*, https://countryeconomy.com/countries/compare/estonia/usa [https://perma.cc/RQY7-BZGH] (last visited May 11, 2022).

[95] Katherine Schaeffer, *What we know about online learning and the homework gap amid the pandemic*, PEW RES. CTR. (Oct. 1, 2021), https://www.pewresearch.org/fact-tank/2021/10/01/what-we-know-about-online-learning-and-the-homework-gap-amid-the-pandemic/ [https://perma.cc/BFJ2-UMUN].

[96] Emily A. Vogels, *Some digital divides persist between rural, urban and suburban America*, PEW RES. CTR. (Aug. 19, 2021), https://www.pewresearch.org/fact-tank/2021/08/19/some-digital-divides-persist-between-rural-urban-and-suburban-america/ [https://perma.cc/A2SW-PFG5].

[97] Andrew Perrin & Sara Atske, *Americans with disabilities less likely than those without to own some digital devices*, PEW RES. CTR. (Sept. 19, 2021), https://www.pewresearch.org/fact-tank/2021/09/10/americans-with-disabilities-less-likely-than-those-without-to-own-some-digital-devices/ [https://perma.cc/7ULX-Z3NJ].

also rely on the USPS for critical goods, such as medications for the disabled and the elderly.[98] The Trump Administration's moves to disparage and further starve the USPS of resources did not help with this inequity problem.[99] Fortunately, with recent legislation providing it with much-needed funds and paving the way for future reforms, the USPS appears to be on track to recover.[100] If the U.S. government were to distribute its new national ID cards through the mail, the USPS's role will become even more crucial because failure to properly deliver the IDs will be tantamount to exclusion.

Keeping these equity challenges in mind, the U.S. government should ensure that every eligible individual seeking to sign up to get an ID can do so easily. Post offices already process passport applications and renewals; they could also take on the new national ID. Federal buildings, such as district courthouses, could also offer national ID issuance and replacement services. The government could explore offering additional services for rural areas where post offices and federal buildings are scarce.[101] Assuming a similar form factor to the Estonian e-ID card, the new ID cards will need to be distributed with card readers.[102] As public adoption of the new ID becomes more widespread, market solutions may emerge that obviate the need for card readers. For example, personal computer manufacturers could offer computers

---

[98] Catherine Kim, *If the US Postal Service fails, rural America will suffer the most*, VOX (Apr. 16, 2020, 8:20 AM), https://www.vox.com/identities/2020/4/16/21219067/us-postal-service-shutting-down-rural-america-native-communities [https://perma.cc/3UZM-Y982]; Jack Healy, *The Chick's in the Mail? Rural America Faces New Worries With Postal Crisis*, N.Y. TIMES (Aug. 21, 2020), https://www.nytimes.com/2020/08/21/us/postal-service-mail-rural.html [https://perma.cc/PNB5-AYYS].

[99] Philip Rucker, Josh Dawsey, & Ashley Parker, *Tracing Trump's Postal Service obsession—from 'loser' to 'scam' to 'rigged election,*' WASH. POST (Aug. 15, 2020), https://www.washingtonpost.com/politics/trump-post-office-mail-vote/2020/08/15/27a2ffd4-de5f-11ea-809e-b8be57ba616e_story.html [https://perma.cc/CHU6-G3SF].

[100] David Shepardson, *Biden signs U.S. Postal Service financial reform bill*, REUTERS (Apr. 6, 2022, 6:45 PM), https://www.reuters.com/world/us/us-postal-service-plans-raise-prices-first-class-mail-2022-04-06/ [https://perma.cc/H3CT-E9ZN].

[101] *See* Kevin Drum, *The Quick Way to End the Vote-Fraud Wars? A National ID Card*, MOTHER JONES (July 2012), https://www.motherjones.com/politics/2012/07/national-id-card-voter-fraud-solution/ [https://perma.cc/HKG9-UEAJ] ("Live in a small town that has neither? No problem—roving ID-mobiles roll through each village and hamlet once every month or two.").

[102] Hammersley, *supra* note 70 (describing the process of becoming an e-resident of Estonia, which includes going to an Estonian police station to pick up a box containing "[the author's] card, a USB reader, a sealed envelope with [the author's] PIN code and an invitation to visit a particular URL.").

with the card readers built in as a feature.[103] As existing REAL ID card readers can only read bar codes,[104] the government could set an appropriate phasing period during which legacy infrastructure is transitioned to the new public key infrastructure, and both REAL ID and the new ID are accepted for commercial travel. The government could incentivize and accelerate the transition by not accepting REAL ID for accessing government services administered over the Internet.

K. Safeguards and Rules

The new national ID system should address the fears of surveillance, exploitation, and exclusion discussed in Part II through both thoughtful design of the system itself as well as rules that govern the use of national IDs and the information associated with them.

A key issue related to the fears of surveillance and exploitation that must be addressed is function creep.[105] Function creep occurs when a system or technology's use is expanded beyond its original purpose,[106] and in the context of information collection and management, beyond the scope of consent. For example, a national ID could collect people's fingerprints with their consent to prevent benefit fraud. Without proper rules and accountability measures in place, these fingerprints could also be used by law enforcement personnel, who could query the fingerprint database for potential matches to suspected criminals.[107]

While there are statutory and constitutional protections in place that may prevent the most egregious abuses of a government-owned national ID database, they do not go far enough to prevent the wide variety of potential abuses, especially in the context of law enforcement. For example, the Privacy Act of 1974 precludes government agencies from collecting information about First Amendment activities without statutory authorization or consent by the

---

[103] *See, e.g.,* Willie S. Fancher, *List of Laptops with CAC Smart Card Readers (Built-in)*, FEATURE LENS, https://featurelens.com/laptops-with-cac-smart-card-readers/ [https://perma.cc/K89J-CYCN] (last visited May 16, 2022).

[104] The REAL ID Act requires that IDs follow an International Organization for Standardization (ISO) technical standard for "bar code symbology." 6 CFR § 37.19, *Machine readable technology on the driver's license or identification card*, https://www.law.cornell.edu/cfr/text/6/37.19 [https://perma.cc/YW9W-72TL].

[105] For a general discussion on defining "function creep," *see* Bert-Jaap Koops, *The Concept of Function Creep*, 13 L. INNOVATION & TECH. 29 (2021).

[106] *Id.*

[107] Amba Kak et al., *Bringing Openness to Identity: Technical and Policy Choices For Open National ID Systems*, THE MOZILLA BLOG (Jan. 2020), https://blog.mozilla.org/netpolicy/files/2020/01/Mozilla-Digital-ID-White-Paper.pdf [https://perma.cc/8R48-H7GB].

individual, and limits collection of personal information to "such information . . . as is relevant and necessary to accomplish a purpose of the agency."[108] Information sharing with any other entity must be preceded by the agency making "reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."[109] Critically, however, the Privacy Act exempts law enforcement activity from its numerous restrictions, leaving the fear of surveillance largely unaddressed.[110] There have indeed been reports of certain agencies compiling information on citizens—even those not suspected of any crimes.[111] Similarly, the Fourth Amendment protection against unreasonable searches and seizures could be overcome by a court determination that queries in a database are reasonable warrantless searches.[112] Alternatively, the court could find that such database queries are not searches at all because the data was furnished voluntarily to a government agency and are government-owned much like the information voluntarily provided in a driver's license application.[113] Finally, neither the Privacy Act nor the Fourth Amendment apply to non-government actors, leaving potential abuses by the private sector and the fear of exploitation unaddressed.

Technical safeguards in the new national ID system could certainly alleviate some of these worries. The new system should be set up with key protections incorporated into its design.[114] Ensuring transparency is critical to mitigate risks of function creep and exploitation of the data within. Employing blockchain technology could provide individuals with transparency in access: data subjects should be able to know when new information is appended to their record in the national ID system, when existing information has been updated, and when public or private entities query their data. Building the ID system on open-source infrastructure and allowing it to be technically auditable by independent third parties is a key part of transparency, ensuring trust, security, and inclusion.[115] An open-source approach also offers

[108] The Privacy Act, 5 U.S.C. § 552a(e)(1) and (7).
[109] *Id.* at (e)(6).
[110] The Privacy Act, *supra* note 108, at (a)(8)(B)(iii), (b)(7) (exempting law enforcement activities from the definition of "matching programs" and the restriction on dissemination of records).
[111] *See, e.g.*, Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, WALL ST. J. (Dec. 13, 2012), https://www.wsj.com/articles/SB10001424127887324478304578171623040640006 [https://perma.cc/JUC8-YUQL].
[112] *See* Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1097 (1996).
[113] The Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721–25, allows drivers' personal information to be shared with law enforcement agencies; Froomkin, *supra* note 28, at 303.
[114] Froomkin, *supra* note 28, at 310.
[115] Kak et al., *supra* note 107.

advantages in cost efficiency and longevity—proprietary software will almost always be subject to a private company's capacity for continued support and patching.[116] Finally, closely related to transparency is control: Individuals should have the right to access their own data, to contest and correct errors, and to opt out of certain uses of their ID. Control over one's data is essential to monitor against risks of function creep, unsanctioned data collection, abusive profiling, and discriminatory treatment.[117]

No number of technical safeguards in the design of the system can prevent a determined bad actor from misusing the system. The implementation of the national ID system should therefore be accompanied by rules that appropriately restrict the abuse of the system. More specifically, the government should condition the use of national IDs by public and private actors on compliance with data protection rules that govern collection, processing, storage, and disclosure—i.e., the full data lifecycle—similar to the ones enforced by the European Union[118] and recently adopted by a few U.S. states.[119] The data protection rules should include provisions for purpose limitation, which restrict the collection and use of data only to those cases where they are compatible with the initial purpose that the data subject has consented to, and provisions for data minimization, which require that only the minimum necessary data should be collected to fulfill the intended purpose.[120] Though these rules may at first face resistance from private companies, a government-issued and verified unique identifier will be too powerful a tool for the private sector to ignore, especially given the unreliability of existing alternatives like the SSN.[121] As Michael Froomkin puts it, "[t]he carrot of lower transactions costs dangled by easy, secure, reliable, and cheap identification might suffice to create market-based incentives to get businesses to accept the stick of adherence to substantive privacy conditions."[122]

---

[116] PRIV. INT'L, *supra* note 16.
[117] Froomkin, *supra* note 28, at 311; Kak et al., *supra* note 107.
[118] GDPR, *supra* note 83.
[119] *E.g.*, The California Privacy Rights Act, CAL. CIV. CODE § 1798.199.40(a) (West 2020) (effective Jan. 1, 2023) (including purpose limitation, data minimization, and some right of access measures, as well as limited private right of action).
[120] *See* GDPR, Art. 5, *Principles relating to processing of personal data*, https://gdpr-info.eu/art-5-gdpr/ [https://perma.cc/KTM6-JJTU] (last visited Apr. 2, 2022); WORLD BANK, *Practitioner's Guide: Data protection and privacy laws*, https://id4d.worldbank.org/guide/data-protection-and-privacy-laws [https://perma.cc/AEN4-BQE6] (last visited Apr. 2, 2022).
[121] John Markoff, *Weakness in Social Security Numbers Is Found*, N.Y. TIMES (July 6, 2009), https://www.nytimes.com/2009/07/07/us/07numbers.html [https://perma.cc/Y9QM-DAHL]; Naylor, *supra* note 47.
[122] Froomkin, *supra* note 28, at 312.

From the government's perspective, shifting from today's fragmented individual privacy law regime to a data protection regime will feel almost familiar, because the Privacy Act is founded on the same Fair Information Privacy Principles (FIPPs) that underlie data protection regimes such as the EU's GDPR.[123] However, the government must also incorporate one major change: the rules governing the use of national ID data should be free of the law enforcement exemptions seen in the Privacy Act. The fear of surveillance and of the government's exploitation of the national ID system for illicit and inappropriate purposes will always linger if the Privacy Act's ban against agencies' disclosure of personally identifiable information does not apply to cases when law enforcement requests the information.[124]

If removing the Privacy Act's law enforcement exemptions from the national ID system is politically infeasible, the rules should improve on the Privacy Act's current exceptions by making law enforcement access more difficult and transparent. Federal privacy statutes often impose additional procedural restrictions such as requiring advance notice to the individual whose information is being accessed, heightening the proof standard from general probable cause by "requiring clear and convincing evidence, tailored showings of relevance, or exhaustion of other methods," or limiting the use of lawfully obtained information, including precluding subsequent transfers or mandating destruction.[125] If the new data protection rules absolutely must have a law enforcement carve-out, similar provisions should be included to ensure that the American people are protected as much as possible from potential abuse of the national ID system by law enforcement. Another possible measure to alleviate the fear of surveillance is using administrative law principles to govern law enforcement agencies as they do other government agencies, for example by requiring notice and comment whenever there is police rulemaking, thereby placing law enforcement policy under the same public scrutiny that other government agencies regularly subject themselves to during their rulemaking processes.[126]

---

[123] DEP'T OF JUST., OVERVIEW OF THE PRIVACY ACT: 2020 EDITION, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction [https://perma.cc/TH3Y-67FR] (last visited May 17, 2022).

[124] The Privacy Act, *supra* note 108, at (b)(7).

[125] *See, e.g.*, CCPA, RFPA, VPPA, and FERPA. For an in-depth discussion of law enforcement exemptions in federal privacy statutes, *see* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 535 (2013).

[126] *See* Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 137-40 (2016); *see also* Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 TEX. L. REV. 1 (2020) (proposing solutions to the information asymmetry problem surrounding policing in the U.S., including broad use of cost-benefit analysis and notice and comment rulemaking).

V. CONCLUSION

There are very real fears of national ID systems being used to surveil, exploit, and exclude the very people they should be helping. Yet it seems strange and ultimately untenable to be so afraid of a national ID system that we end up with nothing, or perhaps worse than nothing – where federal and local government agencies turn to far less-than-ideal solutions, including participation in personal data trafficking enabled by rampant private surveillance. By coupling careful deployment of modern cryptographic technologies with a strong set of data protection rules that bind both the public and private sectors to their requirements, a new U.S. national ID can work as a public tool purposed for the people's prosperity.