Testimony before the
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Task Force on Artificial Intelligence

Hearing on
"I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age"
July 16, 2021

Elizabeth M. Renieris
Professor of the Practice & Founding Director, Notre Dame-IBM Technology Ethics Lab
University of Notre Dame

INTRODUCTION

Thank you to Chair Foster, Ranking Member Gonzalez, and members of this Task Force, for the opportunity to testify before you. My name is Elizabeth Renieris. I am a Professor of the Practice and the Founding Director of the Notre Dame-IBM Technology Ethics Lab at the University of Notre Dame, where I help to develop and oversee projects to promote human values in technology. I am also a Technology and Human Rights Fellow at the Carr Center for Human Rights Policy at the Harvard Kennedy School and a Practitioner Fellow at Stanford's Digital Civil Society Lab, where my research is focused on cross-border data governance frameworks, as well as the ethical challenges and human rights implications of digital identity systems, artificial intelligence (AI), and blockchain and distributed ledger technologies (DLT).

MY WRITTEN AND ORAL TESTIMONIES REFLECT MY OWN PERSONAL VIEWS AND DO NOT NECESSARILY REFLECT THOSE OF ANY ORGANIZATIONS WITH WHICH I AM AFFILIATED.

The subject of digital identity is of critical importance to me both personally and professionally. I began my legal career as an attorney working on cybersecurity policy at the Department of Homeland Security and would later learn that my personal information was compromised, alongside the information of more than 22 million other Americans, in the now infamous "OPM hack." More than a decade later, I continue to receive regular alerts from my government-appointed identity monitoring service, notifying me that my social security number, email address, or other information may have been used by an unauthorized party or service.

I went on to practice law on three continents, focused on the data protection and privacy challenges raised by new and advanced technologies, with an emphasis on financial technologies (fintech). As the Founder and CEO of the law and policy consultancy HACKYLAWYER, I have had the opportunity to advise the World Bank, the U.K. Parliament, the European Commission, industry bodies, startups, and a variety of international organizations and NGOs alike, on the intersection of data

protection, blockchain, AI, and digital identity. I am also working on a forthcoming book that touches on many of these issues, including the future of digital identity.[1]

I am grateful for the opportunity to participate in a hearing on this important topic and delighted to be joined by esteemed colleagues from organizations which I have actively participated in, including the Better Identity Coalition and Women in Identity.

1. DIGITAL IDENTITY IS BECOMING CRITICAL INFRASTRUCTURE.

Digital identity is often defined as "a collection of electronically captured and stored identity attributes that uniquely describe a [real] person within a given context and are used for electronic transactions."[2] In reality, it is a much more complicated concept with social, technical, political, and economic dimensions.[3] As remote and in-person interactions and transactions increasingly have a digital component, such as the use of a smartphone or other device, digital identity is becoming both more ubiquitous and more complex across all dimensions.

As laid bare by the Covid-19 pandemic, we are increasingly reliant on digital tools and services to interact and transact, whether for purposes of work, school, access to healthcare, banking, or government services, and in nearly all aspects of our lives. Unlike when we interact or transact in person, we have limited visibility into who or what is on the other end of a digital interaction or transaction.

Critical infrastructure describes "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[4] Information and ccommunications technology (ICT), energy grids, transportation networks, and financial services are all critical infrastructure. As these sectors are digitized, automated, and algorithmically and computationally manipulated, they increasingly depend on secure digital identity.

Even before the pandemic, vulnerabilities in digital identity systems contributed to everything from election interference[5] to high-profile ransomware attacks, cryptocurrency theft,[6] and network outages, all by exploiting identity-related vulnerabilities. For example, the Colonial Pipeline attackers were able to use a single compromised password to infiltrate a legacy virtual private network (VPN) without multi-factor authentication (MFA) in place.[7]

---

[1] Elizabeth M. Renieris, *A Future Beyond Data: A Human Approach to Digital Governance* (MIT Press, 2023).
[2] *See* "Mobile Identity: Enabling the Digital World 2020," *GSMA* (First Ed. January 2020), available at https://www.gsma.com/identity/resources/report-mobile-identity-enabling-the-digital-world (hereinafter "GSMA Report").
[3] Digital identity is a sociotechnical concept with political and economic dimensions. *See* José van Dijck and Bart Jacobs, "Electronic identity services as sociotechnical and political-economic constructs," *New Media and Society*, Vol. 22(5), 896-914 (2020), https://journals-sagepub-com.ezp-prod1.hul.harvard.edu/doi/pdf/10.1177/1461444819872537.
[4] "Critical Infrastructure Sectors," *Cybersecurity and Infrastructure Security Agency*, https://www.cisa.gov/critical-infrastructure-sectors.
[5] *See* Ellen Nakashima and Shane Harris, "How the Russians hacked the DNC and passed its emails to WikiLeaks," *The Washington Post*, July 13, 2018, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.
[6] *See, e.g.,* Ellen Nakashima, "U.S. accuses three North Koreans of conspiring to steal more than $1.3 billion in cash and cryptocurrency," *The Washington Post*, February 17, 2021, https://www.washingtonpost.com/national-security/north-korea-hackers-banks-theft/2021/02/17/3dccf0dc-7129-11eb-93be-c10813e358a2_story.html.
[7] *See* Stephanie Kelly & Jessica Resnick-ault, "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators," *The Verge*, June 8, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

As we evolve into a world with the "internet in everything" with ever-more internet-of-things (IoT) devices, sensors, networked technologies, and other connected systems, and as the digital becomes the built environment, these vulnerabilities will exponentially increase.[8] Without secure, reliable, and trustworthy digital identities for people, entities, and things, this new cyber-physical reality will subject people and society to attacks, threatening individual safety and national security alike.[9] In this way, *secure digital identity is becoming critical infrastructure*.

At the same time, as dominant technology companies like Google, Apple, Facebook, Amazon, and Microsoft pursue new revenue streams in healthcare, education, financial services, transportation, and more—sectors that include critical infrastructure—the reach of their digital identity infrastructure also expands correspondingly.[10] These companies also exert direct control over the systems and tools needed for digital identity services more generally. For example, with more than 99% of the global market share for smartphone and mobile operating systems combined, Apple and Google's recent introduction of mobile digital identity wallets makes them dominant players in the digital identity space.

Privately owned and operated digital identity systems feature profit-maximizing business models and are driven by commercial incentives that may threaten the privacy, security, and other fundamental rights of individuals and communities.[11] They also tend to incorporate new and advanced technologies, such as AI, machine learning (ML), and blockchain, that are not well understood and often not subject to sufficiently clear legal or governance frameworks. In order to engender trust, safety, and security in the digital ecosystem, we need trustworthy, safe, and secure digital identity. And in order to engender trust, safety, and security in our society, we need to deploy it ethically and responsibly.

2. THE FEDERAL GOVERNMENT MUST LEAD ON STANDARDS FOR DIGITAL ID.

Recognizing the growing importance of digital identity as critical infrastructure and seeking to reign in the power of large corporations over it, governments in other countries and jurisdictions, including the European Union, United Kingdom, Canada, Australia, New Zealand, and elsewhere are prioritizing efforts to design and build the infrastructure needed to support robust digital identity.[12]

Not to be confused with mandatory national identity schemes linked to civil registration and vital statistics (CRVS), these are instead digital-first identity solutions that provide a public infrastructure to access digital products and services in the public and/or private sectors. For example, the European Commission has stated, "A universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them,"

---

[8] *See* Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven: Yale University Press, 2020).
[9] *See, e.g.*, Eileen Donahoe, "The Need for a Paradigm Shift on Digital Security," *Centre for International Governance Innovation*, https://www.jstor.org/stable/pdf/resrep05241.10.pdf.
[10] *See, e.g.*, Mike Orcutt, "The radical idea hiding inside Facebook's digital currency proposal," *MIT Technology Review*, June 25, 2019, https://www.technologyreview.com/2019/06/25/800/how-facebooks-new-blockchain-might-revolutionize-our-digital-identities/; Emil Protalinski, "Google is bringing Electronic IDs to Android," *Venture Beat*, May 9, 2019, https://venturebeat.com/2019/05/09/google-is-bringing-electronic-ids-to-android/; Bobby Allyn, "Apple iPhones Can Soon Hold Your ID. Privacy Experts Are On Edge," *NPR*, June 12, 2021, https://www.npr.org/2021/06/12/1005624457/apple-iphones-can-soon-hold-your-id-privacy-experts-are-on-edge.
[11] *See* "Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom," *ACLU* (May 2021), https://www.aclu.org/news/privacy-technology/digital-ids-might-sound-like-a-good-idea-but-they-could-be-a-privacy-nightmare/.
[12] *See* Rob Laurence and Ewan Willars, "A Blueprint for National and International Oversight of the Digital Identity Market," *Open Identity Exchange* (March 2020), https://canada-ca.github.io/PCTF-CCP/docs/RelatedPolicies/Blueprint-for-National-International-Oversight-of-the-Digital-Identity-Market-March-2020.pdf.

acknowledging the importance of providing an alternative to privacy-invasive options like "login with Facebook/Google."[13]

Even as we have hundreds of frameworks for ethical AI principles,[14] we lack any for digital identity systems in particular. In order to remain competitive globally, avoid enclosure of the public sphere through privately owned and operated digital identity infrastructure, and protect the civil and human rights of Americans, the federal government must take the lead in shaping technical, commercial, legal, and ethical standards for the design, development, and deployment of digital identity systems as critical infrastructure. The *Improving Digital Identity Act* is a good first step in that direction.[15]

Such standards must not only include best practices with respect to the privacy and security of data, but also measures for fairness, transparency, and accountability on the part of entities and organizations designing and deploying the technology, strong enforcement and oversight mechanisms, and adequate remedies and redress for the people impacted. They must also address power asymmetries, the risks of exclusion and discrimination, and specifically address the use of AI, blockchain, and other emerging technologies, by bringing a wide array of voices to the drafting table.

3. DIGITAL ID STANDARDS MUST ADDRESS EMERGING TECHNOLOGIES.

AI/ML in digital identity

Emerging technologies such as AI and blockchain are increasingly used in the context of digital **identity and access management (IAM)**, including for **identity verification (IDV)** and **authentication**. **Verification** (or **proofing**) is typically a one-time process used to onboard a customer or create an account for an individual by linking a unique individual to an identity document or identity information. **Authentication** is typically a recurring process by which to determine that a previously verified individual is who they say they are on the basis of one or more **factors of authentication**.

Low assurance environments, like logging into a social media account, may require simple login credentials, such as a username and password. Where more assurance is required, such as accessing a benefits portal, two or more factors may be required, such as login credentials and a code sent to a verified phone number associated with the account. Even higher assurance environments, such as financial services, may require biometrics such as a fingerprint, face, or voice, or (increasingly) behavioral biometrics,[16] many of which are known to exhibit both racial and gender bias.[17]

AI and ML systems are frequently used to process biometrics for IAM. For example, remote, AI-powered IDV through the use of **biometric facial verification** allows individuals to prove their identity by providing an image of their identity documents (e.g., a driver's license or passport) and a live picture or video of their face. Machine learning models are then used to determine the likelihood that those

---

[13] *See* "Shaping Europe's Digital Future," *Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions*, COM(2020) 67 Final (February 19, 2020), https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf.
[14] *See* Jessica Fjeld and Adam Nagy, "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI," *Berkman Klein Center for Internet & Society*, January 15, 2020, https://cyber.harvard.edu/publication/2020/principled-ai.
[15] *Improving Digital Identity Act of 2021*, H.R. [ ], 116th Congress (2021), https://foster.house.gov/sites/foster.house.gov/files/Digital%20Identity%20Act%20of%202020%20%28FOSTER_065_xml%29.pdf.
[16] *See* GSMA Report, *supra* note 2.
[17] *See* Joan Palmiter Bajorek, "Voice Recognition Still Has Significant Gender Biases," *Harvard Business Review*, May 10, 2019, https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.

documents are authentic by extracting data from the document and attempting to detect any digital or other manipulations of the photo, such as changes to the name or date of birth. Once the identity document is determined to be authentic, the model is then used to perform a biometric-based **facial similarity check** to determine whether the facial image on the document matches the face in the selfie or live video of the individual presenting it. If the document is genuine and the faces match, the person passes the IDV check. Machine learning is meant to take these inputs and produce an output at a level that is as good as or better than a human check.[18]

In order to be reliable and accurate, AI-powered digital identity solutions require a lot of data—typically sensitive, personal data such as facial images and other biometrics. A training set of millions of images of faces is required for facial similarity models, which are only as good as the training data and require continuous monitoring and correction.[19] Mistakes in AI used for IDV can lead to significant consequences, such as the denial of access to services, especially when there is no analog or physical alternative, which is increasingly the case. This challenges core data protection and privacy principles such as data minimization, purpose and use limitations, storage limitations, and data integrity and quality principles, among others, while introducing new risks of bias, discrimination, and exclusion.[20]

While we tend to focus on the data privacy and security features of a specific AI-powered ID tool, we often ignore the privacy and security implications for people whose personal data and faces were used to build and train those tools and models in the first place. This creates an asymmetry between the privacy of individuals used as inputs for the AI and the beneficiaries of any tools that incorporate it. Moreover, as a result of complex supply chains of personal data use, the entities designing and building AI-based identity solutions are often not the ones using or deploying them. Without a direct relationship to the companies designing and building these tools, the chain of responsibility and accountability for privacy and security often breaks down, leaving individuals with limited visibility, control, or recourse over how their information is used.[21] This challenges core data protection and privacy principles, including fairness, transparency, and accountability, among others.

Blockchain/DLT in digital identity

Blockchain or DLT is also increasingly being used for IAM activities, including remote IDV and authentication. DLT is a record of transactions that exists and is simultaneously updated on every computer in a network. A blockchain is a subset of DLT in which "blocks" of transactions are cryptographically linked together in a tamper-proof, immutable, append-only record. Communities within standards organizations, such as the World Wide Web Consortium (W3C)[22] and Decentralized Identify Foundation (DIF),[23] and other standards-adjacent groups are working on developing technical standards for blockchain-enabled **decentralized identity**, sometimes also referred to as **self-sovereign identity (SSI)**.

---

[18] *See* Neal Cohen, "The Ethical Use of Personal Data to Build AI Technologies: A Case Study on Remote Biometric Identity Verification," *Carr Center Discussion Paper* (April 2020), https://carrcenter.hks.harvard.edu/files/cchr/files/200228_ccdp_neal_cohen.pdf.
[19] *See, e.g.*, Omkar M. Parkhi, Andrea Vedaldi, and Andrew Zisserman, *Deep Face Recognition*, University of Oxford (2015), https://www.robots.ox.ac.uk/~vgg/publications/2015/Parkhi15/parkhi15.pdf.
[20] *See, e.g.*, "Big Data: A Tool for Inclusion or Exclusion: Understanding the Issues," *Federal Trade Commission* (January 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[21] This complexity is often compounded by the practice of "white-labeling" or making a technology appear as though it was built and operated by the company making the service available.
[22] W3C DID Working Group, https://www.w3.org/2019/did-wg/.
[23] Decentralized Identity Foundation, https://identity.foundation.

While the technical specifications are complex and constantly evolving, the basic idea is to use a blockchain or distributed ledger as an authoritative record by which to track and prove ownership over one or more **decentralized identifiers (DIDs)** through the use of decentralized public key infrastructure (DPKI). These DIDs are then used to manage the exchange of cryptographically verifiable digital credentials consisting of one or more claims about an individual, known as **verifiable credentials (VCs)**.[24] An entity known as an **issuer** can create or "issue" a VC about an individual (who is the **subject** of that VC) to a **holder**, who will "hold" or store the VC in a mobile or web-based **digital wallet**.[25] Through these wallets (and corresponding wallet software), individuals can use DIDs to establish and manage connections to other individuals and entities, and present VCs to entities who rely on them, known as **verifiers**.

At its core, blockchain is an accounting technology. It is a transparent, auditable, traceable, and permanent record of transactions, which makes it a popular technology for cryptocurrency and supply chain management.[26] But these same properties make it a high-risk technology to use in connection with personal identity management—*blockchain is anything but private by design*. Conceptually, blockchain remains difficult (if not impossible) to reconcile with core data protection principles such as data minimization (by automatically replicating data across all nodes in a network), storage limitation (by indefinitely storing data), and certain rights related to erasure or the restriction of processing (due to its immutable nature), among others.[27]

To resolve these tensions, blockchain-based identity management relies heavily on various methods of pseudonymization, anonymization, and encryption, particularly for transactional metadata stored on the ledger. Even as new and innovative technical solutions are employed to pseudonymize or anonymize transactional data stored on a distributed ledger, we have countless examples of how inadequate pseudonymization and anonymization techniques can be and how even aggregated, anonymous data can put people and national interests at risk.[28] And even before quantum computing breaks modern encryption,[29] metadata is also increasingly capable of identifying individuals as it gets combined and cross-referenced with other data.

Finally, most blockchain networks still struggle with speed, reliability, and availability.[30] In fact, rather than eliminating single points of failure (as is typically alleged by technology promoters), the blockchain or ledger itself can become an even more pronounced single point of failure in a digital ID system (e.g., if the network is down or transactions cannot be processed, the entire system could malfunction or fail). This is highly problematic from the perspective of digital identity as critical infrastructure.

---

[24] *See* "Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web," *W3C Recommendation* (November 19, 2019), https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.

[25] The subject and holder may or may not be the same individual. In fact, proving that the holder of a credential is that subject of that credential is one of the biggest unsolved challenges of the decentralized or self-sovereign approach to digital identity.

[26] It is also the backbone of China's central bank digital currency (CBDC), which is legitimately raising concerns about privacy and surveillance. *See, e.g.*, Akram Keram, "China wants to take the entire country cashless—and surveil its citizens even more closely," *The Washington Post*, March 2, 2021, https://www.washingtonpost.com/opinions/2021/03/02/china-digital-yuan-currency-surveillance-privacy/.

[27] *See* Elizabeth M. Renieris, "Forget erasure: why blockchain is really incompatible with the GDPR," *Berkman Klein Center for Internet & Society*, September 23, 2019, https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-really-incompatible-with-the-gdpr-9f60374e90f3.

[28] For example, the fitness tracking app Strava made headlines for revealing the location and activities of U.S. military personnel around clandestine bases in Syria when it published anonymized heatmaps of popular running routes. *See* Zack Whittaker, "How Strava's 'anonymized' fitness tracking data spilled government secrets," *ZDNet*, January 29, 2018, https://www.zdnet.com/article/strava-anonymized-fitness-tracking-data-government-opsec/.

[29] *See* Aleksey K. Fedorov, Evgeniy O. Kiktenko, and Alexander I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature,* November 19, 2018, https://www.nature.com/articles/d41586-018-07449-z.

[30] *See, e.g.,* David Floyd, "When Blockchains Go Down: Why Crypto Outages Are on the Rise," *Coindesk*, September 23, 2018, https://www.coindesk.com/when-blockchains-go-down-why-crypto-outages-are-on-the-rise.

4. WE NEED GUARDRAILS FOR THE *USE* OF DIGITAL ID SYSTEMS.

Despite the growing ubiquity and importance of digital identity in all facets of life, IAM continues to be a highly technocratic field. Democratic processes and decision-making about the use of emerging technologies for digital identity are often outsourced to technical standards bodies, the private sector, and industry consortia. I have directly participated in many of these groups and I can assure you that they lack all manner of diversity. They are overwhelmingly white, western, and male, and dominated by a veneration for *technical* proficiency (defined as computer science and engineering skills) over and above all other skills, including law and policy expertise. As a result, it can be difficult for the designers and developers of these technologies to imagine or anticipate the risks to people and communities. For example, there tends to be a vast divide between what technologists mean by *privacy* in this context, as compared to how law and policymakers (or the public) think about it.

Privacy is a powerful concept rooted in constitutional and human rights law that has to do with the inviolability of the individual and preventing unlawful interferences with the individual's private life. It is necessary for the exercise and enjoyment of other fundamental rights, including the freedom of thought and conscience, for individual autonomy, and as protection against disparate treatment and discrimination. Unfortunately, in my experience, the technical communities designing and building digital identity standards and systems use the term *privacy* to refer to a kind of mathematical exercise in secrecy and/or anonymity. *Secrecy* in the sense of withholding certain data points in a given interaction or transaction, e.g., industry frequently gives the example of proving that someone is over 21 without revealing their actual date of birth. And *anonymity* in the sense of the degree to which an individual is identifiable or anonymous in a given digital interaction or transaction.[31]

Moreover, digital identity providers often tout their use of zero knowledge proofs or other **privacy-enhancing technologies (PETs**) in designing and building digital identity solutions. While PETs can be helpful for achieving legal compliance as part of *privacy by design* efforts, many of these technologies and methods remain untested and unproven at scale, while introducing levels of complexity that can actually compromise their stated objectives.[32] As digital identity becomes critical infrastructure, we cannot view *privacy* through such a narrow, mathematical lens. Instead, we must consider the impact of digital identity technologies as part of *complex socio-technical systems* with serious consequences for individuals, communities, and society at large[33]—repercussions that far exceed the scope of any narrow technical specifications of a single app, tool, or service.

When viewed as part of socio-technical systems, attribute-based identity schemes such as decentralized identity or SSI raise much broader concerns about equity, inclusion, and discrimination, as well as privacy. For example, the data formats and schema used in these systems can determine whether an attribute such as gender is expressed as a mere binary (i.e., male and female) without alternatives. Moreover, when certain attributes are required or encoded, they run the risk of excluding individuals without those attributes. Perhaps less obviously, the use of PETs and the appearance of privacy-preserving design choices can make these systems appear less intrusive, which could make businesses,

[31] There are also many reasons why an individual might want to share their data, reveal their identity, or otherwise be known in the context of a commercial or non-commercial relationship. Additionally, hiding might be a privilege that is unavailable to those whose access to services is conditioned on sharing personal information or identity information. This is another reason why who is at the table building and shaping these tools and standards matters.
[32] While they can be helpful for achieving legal compliance, privacy-enhancing technologies (PETs) are no panacea and not without significant risks. *See, e.g.*, Elizabeth Renieris, "Why PETs (privacy-enhancing technologies) may not always be our friends," *Ada Lovelace Institute*, April 29, 2021, https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/.
[33] *See* van Dijck and Jacobs, *supra* note 3.

governments, and other entities feel less restricted to request identity information in contexts where it was previously unacceptable or unnecessary.[34]

When we move through the physical world, we are rarely asked to identify ourselves. Presenting a government-issued ID is the exception, reserved for high-risk situations like boarding an international flight. But as the market for digital ID systems and solutions grows, and as everything from online to in-person services increasingly has a digital component, we are at risk of flipping that paradigm and of requiring people to identify themselves in all manner of settings and situations. Increasingly cheap, efficient, and "seamless" forms of digital identity, such as contactless payments and palm scanning technologies, could also create a fictious need for individuals to identify themselves in contexts where such a need did not previously exist.[35] If we are not careful and deliberate about it, we might go from a situation in which identity is the *exception* to one in which identity becomes the *rule.*

As I argue in a forthcoming book for MIT Press, just because the *data* in a system is private and secure, does not mean that the *people* implicated by the system are protected. For example, just because the data doesn't leave your phone, does not mean you cannot be controlled or manipulated through the use of on-device machine learning algorithms and other computational processes.[36] Reducing the risks of ID systems to questions of mere *data* security and privacy does little to protect the rights of *people*. In fact, it can create a false sense of safety and security that actually puts people at heightened risk. Existing legal frameworks are ill-equipped to address these challenges. To avoid the erosion of privacy through persistent and ubiquitous identification,[37] we will also need to articulate and implement *clear guardrails around the use of these systems*, including when and why identity can be required.[38]

5. WE NEED A PUBLIC OPTION THAT IS NOT DRIVEN BY PROFIT MAXIMIZATION.

Right now, there are few commercial incentives around the use of your physical, government-issued identity documents. In general, no one knows when you use them or gets paid when you do (e.g., the DMV isn't typically notified or paid when you use your license to purchase alcohol). In contrast, digital identity schemes typically have commercial and technical incentives that are very different from in-person, manual processes. The use of emerging technologies for digital identity management risks transforming identity from something *relational* (established in the context of government to citizen, or business to customer) into something *transactional*—turning identity into a commodity.

In fact, digital identity is big business and growing bigger every day. The global market for IAM is expected to reach $29.79 billion by 2027,[39] while the global IDV market is expected to reach $17.8 billion by 2026.[40] Cloud-based authentication or identity as a service (IDaaS) offerings based on AI/ML

[34] *See* Merel Koning, et al, "The ABC of ABC: An Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity," *Internet, Law & Politics: A Decade of Transformation* (July 2014), 357-374, http://www.cs.ru.nl/~jhh/publications/abc-of-abcs.pdf.
[35] *See, e.g.,* James Vincent, "Amazon's palm reading starts at the grocery store, but it could be so much bigger," *The Verge*, October 1, 2020, https://www.theverge.com/2020/10/1/21496673/amazon-one-palm-reading-vein-recognition-payments-identity-verification.
[36] *See, e.g.*, Michael Veale, "Privacy is not the problem with the Apple-Google contact-tracing toolkit," *The Guardian*, July 1, 2020, https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights.
[37] *See* "Annual Digital Lecture 2020: The death of anonymity in the age of identity," *The National Archives* (February 2, 2021), https://media.nationalarchives.gov.uk/index.php/annual-digital-lecture-2020-the-death-of-anonymity-in-the-age-of-identity/.
[38] Akin to laws that limit the swiping or scanning of physical drivers licenses by retailers for specified purposes. See, e.g., John T. Cross, "Age Verification in the 21st Century: Swiping Away Your Privacy," 23 J. Marshall J. Computer & Info. L. 363 (2005).
[39] *See* "Identity and Access Management Market by Component, by Deployment Model, by Application, Competitive Landscape, by Geography and Forecast," *Verified Market Research* (November 2020), available at https://www.verifiedmarketresearch.com/product/global-identity-access-management-market-size-and-forecast-to-2025/.
[40] *See* "Global Identity Verification Market By Component, By Type, By Enterprise Size, By Deployment Type, By End User, By Region, Industry Analysis and Forecast, 2020 – 2026," *KBV Research* (December 2020).

is one of the fastest growing segments of the market.[41] But just as we are learning the high price to society of the targeted behavioral advertising-based business models that fuel social media and the surveillance economy, we must examine the commercial incentives and revenue models behind digital ID schemes.

While business models vary, digital identity products and services are typically either enterprise grade (B2B) or consumer grade (B2C). For example, the entity building a remote, AI-based IDV tool is typically a vendor to another company providing a product or service to end users. A common business model in this B2B arrangement is a **pay-per-verification** scheme, whereby the AI vendor is compensated per verification check (or per query or API call), or per user in a given time frame (e.g., one month) in the case of IDaaS arrangements.[42] Alternative subscriptions and volume-based pricing models, as well as hybrid arrangements are also possible. Certain commercial arrangements, such as pay-per-verification schemes, could incentivize the overuse of identity systems and even undermine the technical features designed to promote privacy.[43]

Coming up with effective business models and commercial incentives for decentralized identity has been one of the core hurdles to adoption of blockchain-based IAM.[44] For example, incentivizing entities to undertake the investment to be able to issue digital credentials may require certain assurances of recouping those costs and extracting value from those credentials. One common solution proposed for this in the SSI context is to have the verifier pay the issuer of a credential for each verification. As with AI-powered IDV, the verifier pay issuer scheme might incentivize overuse and compromise some of the technical measures taken to protect privacy. Moreover, the digital wallet and other software components that intermediate the use of credentials can make it challenging to compensate parties, while ensuring they are blind to what an individual does with those credentials.

Finally, leaving access to critical digital identity infrastructure to the private sector risks turning safe, secure, and trustworthy digital identity into a luxury good, as has been the case with privacy.[45] For people without access to or the ability to pay for certain technologies, such as the latest smartphone, the growing ubiquity of digital identity could drive increasing exclusion. And for people with access, it may increase their risk of being surveilled, controlled, and manipulated. To prevent exclusion and avoid predatory inclusion, the government also must ensure the availability of a public option that is shaped by civic and democratic values over and above commercial profit motives.

6. WE MUST PREVENT DIGITAL ID FROM BECOMING A TOOL FOR SURVEILLANCE.

Finally, we must avoid building digital identity systems and infrastructure in a way that further expands and entrenches the surveillance state, as do the national identity systems in India or China.[46] Under no circumstances should we think about digital identity as a mandatory, biometric-based national

[41] *See* "$6.5 Bn Identity as a Service Market – Global Forecast to 2024," *PR Newswire*, September 23, 2019, https://www.prnewswire.com/news-releases/6-5-bn-identity-as-a-service-market---global-forecast-to-2024--300923095.html.
[42] *See, e.g.*, "Pricing," iDenfy, https://www.idenfy.com/identity-verification-price/.
[43] For example, where a company pays an IDV provider on a pay-per-verification basis and fails to keep personal data separate from billing-related data, this could compromise the privacy and security of data subjects. This is also true with respect to certain decentralized identity solutions and wallet providers that purport to avoid the "phone home" problem at a technical level, while enabling it at a business level.
[44] *See, e.g.*, SSI Ambassador, "The growth factors of self-sovereign identity," *Medium*, April 13, 2020, https://ssi-ambassador.medium.com/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7.
[45] *See* Adam Clark Estes, "Apple's Newest Luxury Product is Privacy," *Gizmodo*, June 4, 2019, https://gizmodo.com/apples-newest-luxury-product-is-privacy-1835233518.
[46] *See, e.g.*, Nikhil Pahwa, "Thought China was getting all Big Brother? India's not far behind," *Wired*, September 26, 2018, https://www.wired.co.uk/article/india-aadhaar-database-legal-supreme-court.

identity scheme, or as an avenue for social credit scoring our citizens. For public schemes, we should avoid the use of a single, centrally-issued, all-purpose, unique identifier for individuals that can be linked across contexts from employment, to education, healthcare, banking, and more.

While we should of course leverage PETs and aim for privacy and data protection by design and default in our digital identity infrastructure, we should not rely on technological solutions alone to address questions of privacy, security, equity, access, and inclusion because identity is inherently sociotechnical. We must also consider the nature of emerging technologies used in digital ID systems, as well as the commercial incentives and impact of business models implicated.

In addition to building consensus around technical, legal, commercial, and ethical standards for digital identity, we also need to articulate and implement concrete guardrails around the use of identity, whether public or private, including when and how ID can be required. Just as privacy is contextual, we must be able to calibrate our use of digital identity infrastructure, depending on the context and circumstances of a given interaction or transaction, as we do in the physical world.

While safe, secure, and trustworthy identity is critical to instill confidence in an increasingly digital world, we must reject the notion that simply using a digital technology or tool should require us to identify ourselves.

CONCLUSION AND RECOMMENDATIONS FOR CONGRESS

In summary, I would make the following recommendations to Congress when thinking about digital identity policy:

1. We must recognize that **digital identity is becoming critical infrastructure**, as other countries have acknowledged.
2. While industry is racing ahead, the **federal government must lead** to create standards for safe, secure, and trustworthy digital identity. The *Improving Digital Identity Act* is a good first step in that direction.
3. Those standards must address **specific challenges associated with new and emerging technologie**s used in these ID systems, such as AI/ML and blockchain/DLT.
4. Regardless of the technologies leveraged, we need **guardrails around the use of these ID systems**, including when and why ID can be required.
5. We must ensure a **public option** (akin to the eID in Europe), that is not subject to the same commercial incentives as private digital identity schemes.
6. We must **get it right** so that digital identity does not become yet another enabler of **surveillance and control**.

Once again, I appreciate the opportunity to appear before the Task Force and share my perspectives. I look forward to answering any questions you may have.