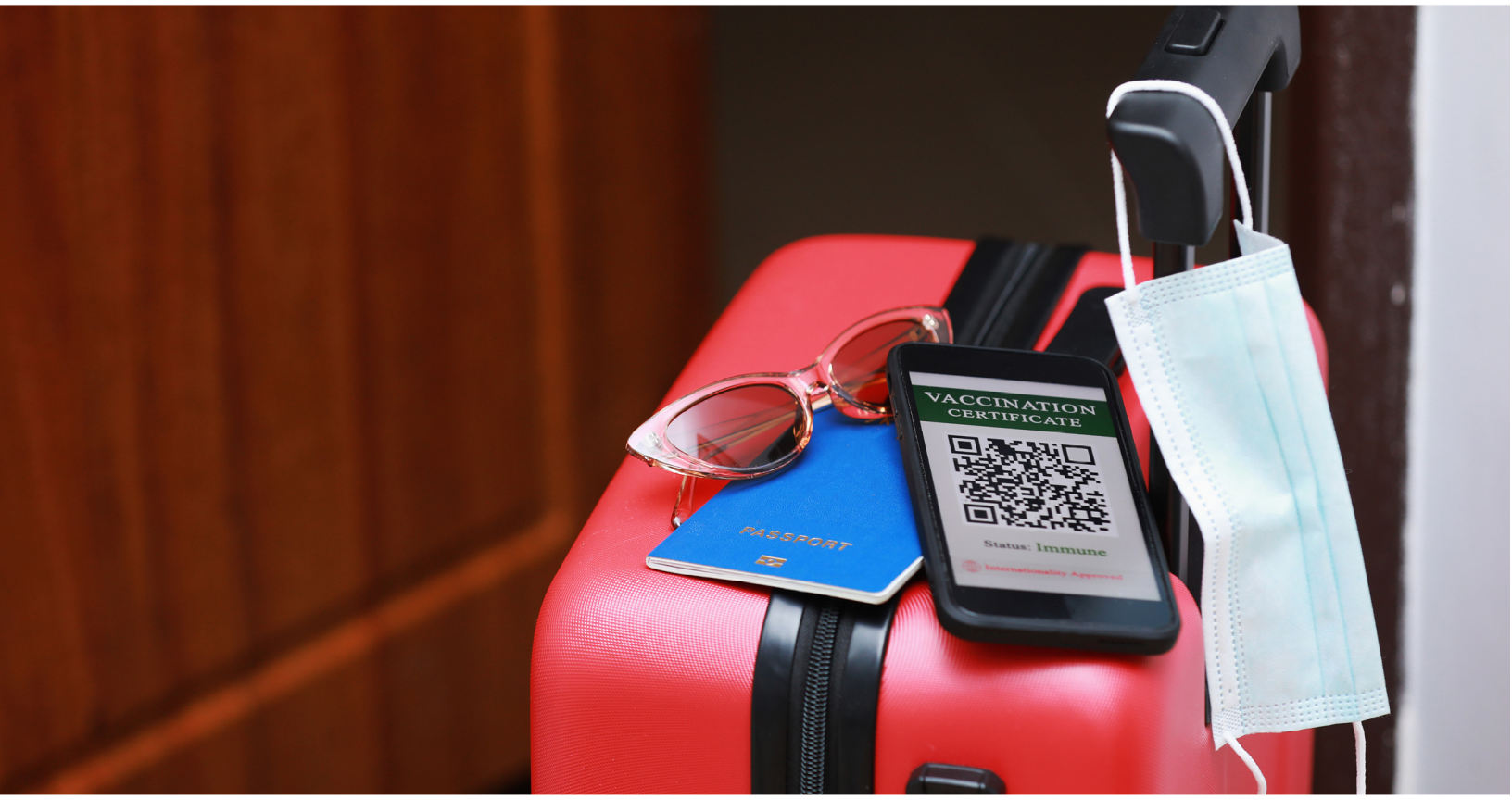
COVID-19 as a Catalyst for Advancement of Digital Identity



LEAD AUTHOR:
Charlyn Ho

CONTRIBUTING AUTHORS:
Samantha V. Ettari, Brandon R. Thompson & April A. Goff

PerkinsCoie.com

Perkins Coie LLP | November 2021

PERKINS COIE

COVID-19 as a Catalyst for Advancement of Digital Identity

Note to Reader: This article discusses areas of law that are developing rapidly, especially given the evolving nature of the COVID-19 pandemic; thus, the reader should check back with the authors as these areas progress. It is not intended to comment on the social value or appropriateness of health certificate systems. Instead, our goal is to address some of the legal considerations that health certificates raise with respect to, and in the context of, the development of a comprehensive system of digital identity management.

Introduction

By restricting and changing the shape of human interaction for over a year, the COVID-19 pandemic rapidly accelerated the digitalization of many services and, in doing so, reinvigorated efforts to establish a cross-contextual digital identity[1] infrastructure.

In today's digital and interconnected world, the ability to verify individuals' identity attributes without resorting to physical identifiers is increasingly important. However, today's digital identity systems are remarkably underdeveloped.[2] As these systems are forced to evolve to address challenges such as those posed by the COVID-19 pandemic, their success will depend upon the effective implementation of at least three digital identity pillars:

1) **trust** (i.e., confidence that an individual's digital identity is what it purports to be and has not been altered);

2) **user-centricity** (i.e., an individual's ability to exercise control over their digital identity, including protecting the privacy of their attributes); and

3) **data security**.[3] Together, these three pillars will form the foundational framework of a robust digital identity system and contribute to the growth and adoption of digital identity systems, as well as determine the systems' utility in accurately identifying individuals and their attributes.

* Charlyn Ho is a partner in the Technology Transactions & Privacy Law practice group at the law firm of Perkins Coie LLP. She counsels clients regarding intellectual property and data protection matters in technology transactions, with a focus on artificial intelligence/machine learning, cloud services, healthcare, and digital identity solutions, among other areas. Charlyn would like to thank Stephanie Duchesneau and Michael Nguyen, 2021 summer associates at Perkins Coie LLP, as well as Heather Dahl, co-founder and CEO of Indicio.Tech, for their important contributions to this paper.

[1] Although there is no singular definition for "digital identity," a number of core features of the concept are widely recognized among academics and multinational organizations. *See, e.g.*, JULIA CLARK ET AL., WORLD BANK GROUP, DIGITAL IDENTITY: TOWARDS SHARED PRINCIPLES FOR PUBLIC AND PRIVATE SECTOR COOPERATION 11 (July 2016) ("Digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions."), https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/file.

[2] *See generally* Usman Ahmed, Daniel Gorfine & Ivy K. Lau, *The U.S. Digital Identity Crisis*, THE REGUL. REV. (Apr. 29, 2021), https://www.theregreview.org/2021/04/29/ahmed-gorfine-lau-us-digital-identity-crisis/ (describing the slow adoption of digital identity systems in the United States); Zara Rahman, *We know what's wrong with digital identification. Here's what works*, THE CORRESPONDENT (Feb. 4, 2020), https://thecorrespondent.com/268/we-know-whats-wrong-with-digital-identification-heres-what-works/300872364100-c78c522e (discussing the challenges of identification systems around the world).

[3] Note that while we view "privacy" as part of user-centricity, we also discuss privacy in tandem with data security, given that privacy and data security are so interconnected.

One of the most timely and well-publicized applications of digital identity is digital health certificates (including those that record vaccination status),[4] which theoretically support post-pandemic recovery by enabling individual users to visit certain locations or undertake certain activities based upon their testing or vaccination status.[5] The potential cross-contextual and cross-jurisdictional uses for health certificates, as well as the significant role that they could play in determining whether an individual can work, travel, access certain locations, etc., have rapidly advanced discussions on how to provide a comprehensive system of digital identity that is built upon the three pillars of trust, user-centricity, and data privacy and security. This paper will explore the necessity of these pillars to the advancement of digital identity systems in general and as applied to health certificates specifically, while also examining legal issues arising out of digital identity systems. This paper does not seek to take a stance on the viability of health certificates or whether they should be adopted, but rather probes how health certificates serve as a catalyst for advancement of digital identity more broadly.

RETURN TO NORMAL AFTER THE COVID-19 PANDEMIC

In early 2020, the world experienced a nearly complete economic and social standstill as public health authorities came to understand the grave risks associated with contracting the coronavirus and the virus's rapid spread around the globe.[6] Ultimately, the COVID-19 pandemic touched nearly every part of our daily existence. Many lost loved ones, as the virus would eventually claim over 4 million lives worldwide.[7] And, in an attempt to curb the rapid transmission of the virus, people all around the world undertook significant changes to their daily modes of life. Travel virtually ground to a halt as public officials endeavored to contain the spread of the virus within their borders.[8] Sporting events were canceled,[9] restaurants shut their doors,[10] schools moved to online learning,[11] and offices in nonessential sectors closed,[12] requiring people to quickly adjust to the new realities of working and learning from home. In-person social gatherings largely came to a halt as well, whether due to social distancing and reduced occupancy orders or personal fear of contracting the virus.

While the virus came in documented waves and we learned more about its communicability and symptoms, public health mandates and guidance shifted, and life showed little promise of returning to normal until the approval of

---

[4] *See, e.g.*, Stephen Davidson, *How Vaccine Passports Could Change Digital Identity*, DIGICERT (June 11, 2021), https://www.digicert.com/blog/how-vaccine-passports-could-change-digital-identity. Notably, however, even the term "vaccine passport" is often amorphous and not without its detractors. *See* Leana S. Wen, *Opinion: Stop calling them 'vaccine passports'*, WASH. POST (Apr. 7, 2021), https://www.washingtonpost.com/opinions/we-need-to-stop-debating-vaccine-passports-and-instead-define-what-we-need-to-reach-normalcy/2021/04/07/47d0b8e0-97b5-11eb-962b-78c1d8228819_story.html. Therefore, for the purposes of this paper, a digital "vaccine passport" is to be understood as any digital identification credential that would enable an entity to validate that the proof-of-vaccination information is accurate as presented and verify that the rightful holder of the proof-of-vaccination information is the person asserting as such.

[5] *Could a Vaccine Passport or Mandate be in Store for Chicago? Top Doc Weighs In*, NBCCHICAGO.COM (Aug. 12, 2021), https://www.nbcchicago.com/news/coronavirus/could-a-vaccine-passport-or-mandate-be-in-store-for-chicago-top-doc-weighs-in/2589103/.

[6] Gary P. Pisano, Raffaella Sadun & Michele Zanini, *Lessons from Italy's Response to Coronavirus*, HARVARD BUS. REV. (Mar. 27, 2020), https://hbr.org/2020/03/lessons-from-italys-response-to-coronavirus.

[7] Figures are based on the World Health Organization's COVID-19 Dashboard as of June 29, 2021 (10:45 EDT), available at https://covid19.who.int/. The dashboard tracks reported cases and deaths, meaning that the virus's actual death count is likely higher than reported.

[8] Amelia Cheatham et al., *The Year the Earth Stood Still*, COUNCIL ON FOREIGN RELATIONS (Dec. 7, 2020), https://www.cfr.org/article/2020-year-earth-stood-still-covid-19.

[9] *See, e.g.*, ESPN News Services, *NCAA tournaments canceled over coronavirus*, ESPN (Mar. 12, 2020), https://www.espn.com/mens-college-basketball/story/_/id/28893285/ncaa-tournaments-canceled-coronavirus.

[10] CAL. DEP'T OF PUB. HEALTH, GUIDANCE ON CLOSURE OF SECTORS IN RESPONSE TO COVID-19 (July 13, 2020), https://www.cdph.ca.gov/Programs/CID/DCDC/Pages/COVID-19/Guidance-of-Closure-of-Sectors-in-Response-to-COVID-19.aspx.

[11] *See generally Strengthening online learning when schools are closed: The role of families and teachers in supporting students during the COVID-19 crisis*, ORG. FOR ECON. COOP. & DEV. (Sept. 24, 2020), https://read.oecd-ilibrary.org/view/?ref=136_136615-o13x4bkowa&title=Strengthening-online-learning-when-schools-are-closed&_ga=2.112088640.519099075.1629062287-732579830.1629062287 (describing the move to online schooling in the wake of the coronavirus pandemic).

[12] Kim Parker, Juliana Horowitz & Rachel Minkin, *How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work*, PEW RES. CTR. (Dec. 9, 2020), https://www.pewresearch.org/social-trends/wp-content/uploads/sites/3/2020/12/PSDT_12.09.20_covid.work_fullreport.pdf.

several coronavirus vaccines in late 2020. To date, three such vaccines have been approved for emergency use in the United States (the Moderna, Pfizer, and Johnson & Johnson vaccines, specifically).[13]

In 2021, governments around the world began rolling out these and other vaccines to their populations, consistent with availability and individual need. However, even well over a year into the pandemic, the success of the vaccine rollout is varied—both within the United States and on an international scale. The United States, home to some of the major vaccine distributors, was among the first nations to procure an adequate supply of doses to fully vaccinate its entire population. However, significant pockets of the population still remain unvaccinated. Elsewhere, availability remains a major issue. Across Africa, for example, only 5.55 percent of the population had received one dose of the vaccine and only 3.27 percent had been fully vaccinated as of September 15, 2021, due in part to low availability of doses as well as limited infrastructural capability for administering the vaccines.[14] In terms of global population, only 30.38 percent had been fully vaccinated as of September 15, 2021.[15] Stark differences in vaccine rollouts mean that many populations around the world remain vulnerable to the continued spread of the coronavirus, especially as new variants emerge.[16]

In terms of global population, only 30.38 percent had been fully vaccinated as of September 15, 2021.

The difference in the public health risk posed by vaccinated and unvaccinated segments of the population raises a number of new policy questions. At issue is how to facilitate the "return to normal" for populations who either have been vaccinated or have antibodies due to a recent coronavirus case, while mitigating the risk of spreading COVID-19. To this end, a number of academics, politicians, and public health officials have argued for the development of a health certificate system, which would enable these low-risk individuals to travel or resume in-person activities while continuing to manage the risks presented by unvaccinated populations.[17]

The United States has largely rejected a mandatory health certificate system to track COVID-19 vaccination status because of the myriad legal and policy issues potentially raised by such a system.[18] These include privacy and security considerations; potential interactions with antidiscrimination laws, particularly for those who cannot get vaccinated for medical or other protected reasons; and potential First Amendment concerns.[19] However, private institutions largely remain free to implement their own vaccine mandates. In July 2021, for example, technology companies Google and Facebook announced that they would require proof of vaccination for employees returning to the companies' in-person facilities, with exceptions for individuals in areas where vaccines are not widely available or who cannot be vaccinated for protected reasons.[20] Around the same time, restaurateur Danny Meyer announced his

[13] Kathy Katella, *Comparing the COVID-19 Vaccines: How Are They Different?*, YALE MED. (last updated Aug. 26, 2021), https://www.yalemedicine.org/news/covid-19-vaccine-comparison.
[14] AFRICA CDC, AFRICA CDC VACCINE DASHBOARD, https://africacdc.org/covid-19-vaccination/ (last visited Sept. 16, 2021).
[15] *Coronavirus (COVID-19) Vaccinations*, OUR WORLD IN DATA (https://ourworldindata.org/covid-vaccinations (last visited Sept. 16, 2021)).
[16] Kathy Katella, *5 Things to Know About the Delta Variant*, YALE MED. (updated Sept. 8, 2021), https://www.yalemedicine.org/news/5-things-to-know-delta-variant-covid.
[17] *See* Kevin Cope & Alexander Stremitzer, *Governments Are Constitutionally Permitted to Provide "Vaccine Passports"—Some May Also be Constitutionally Obligated to Do So*, 62 J. of Nuclear Med. 771 (Apr. 16, 2021); Max Greenwood, *Will vaccine passports be biggest campaign issue of 2022?*, THE HILL (Apr. 2, 2021), https://thehill.com/homenews/campaign/546062-the-biggest-campaign-issue-of-2022-vaccine-passports.
[18] *See* Brett Samuels, *White House rules out involvement in 'vaccine passports'*, THE HILL (Apr. 6, 2021, 1:33 PM ET), https://thehill.com/homenews/administration/546705-white-house-rules-out-involvement-in-vaccine-passports. *But see* Exec. Order No. 14,043, 86 FR 50989 (2021) (requiring that all federal employees receive the COVID-19 vaccination); *Path out of the Pandemic: President Biden's COVID-19 Action Plan*, The White House (issuing a statement requiring all employers with 100+ employees to ensure their workers are vaccinated or tested weekly), https://www.whitehouse.gov/covidplan/ (last visited Oct. 25, 2021).
[19] Mark A. Hall & David M. Studdert, *Perspective "Vaccine Passport" Certification—Policy and Ethical Considerations*, 385 NEW ENG. J. OF MED. e32(1) (Sept. 9, 2021), https://www.nejm.org/doi/pdf/10.1056/NEJMp2104289?articleTools=true.
[20] Sundar Pichai, *Vaccines and our return-to-office plans*, GOOGLE COMPANY NEWS BLOG (July 28, 2021), https://blog.google/inside-google/company-announcements/vaccines-and-our-return-to-office-plans/.

plan to require proof of vaccination for both employees and diners at his New York and Washington, D.C. restaurants.[21]

Other jurisdictions have gone further in embracing health certificate systems that are based on the issuance of a digital credential. For example, the European Union (EU) has introduced the EU Digital COVID Certificate to support travel within the Eurozone.[22] At the intrastate level, New York has developed an Excelsior Pass to support access to participating institutions.[23] These systems have met with mixed acceptance. Both the EU Digital COVID Certificate and the Excelsior Pass remain voluntary for now, though some European countries have begun to mandate digital COVID-19 vaccination certificates for entry into indoor, public spaces.[24] Israel, whose Green Pass system was effectively mandatory for those seeking to access in-person businesses and services, faced a wave of public debate over the system's fairness, which contributed to the system's temporary suspension in June 2021 before its ultimate reinstatement the following month.[25] Complicating matters, while several EU countries have beefed up their COVID-19 protocols, others, such as Norway, have nearly simultaneously lifted all COVID-19 restrictions.[26] As such state-initiated protocols change seemingly day to day and from country to country, some industry-led efforts, including the ID2020 Good Health Pass initiative, are attempting to establish their own interoperable frameworks for COVID-19 credentialing to bridge these gaps.[27]

However, whether private or public, the rollout of vaccination systems and their robustness is partly undercut by the lack of a comprehensive, underlying system for utilizing digital identity. Today, proof of vaccination is generally issued to individuals in the form of a physical paper card.[28] While this physical credential may be adequate to support more limited vaccine mandates, such as those by a particular employer or dining establishment, such credentials have a number of shortcomings. For instance, physical credentials are often more unwieldy than digital counterparts (which can be automatically verified through technical means), track vaccine lot numbers and vaccine administration dates (neither of which are easily authenticated), do not allow for selective disclosure, can be easily lost, and can be easily forged (as is evident by their surging trade on the black market).[29] Moreover, these credentials may be wholly inadequate in the context of more complex systems like the aforementioned EU Digital COVID Certificate and ID2020 Good Health Pass.[30] The EU Digital COVID Certificate requires verification of credentials issued by authorities

[21] Jessica Sidman, *Danny Meyer's DC and NY Restaurants Will Require Indoor Diners and Employees to Show Proof of Vaccination*, WASHINGTONIAN (July 29, 2021), https://www.washingtonian.com/2021/07/29/danny-meyers-dc-and-ny-restaurants-will-require-indoor-diners-and-employees-to-show-proof-of-vaccination/. As of his July 29, 2021, announcement, these plans include Meyer's sit-down establishments, but exclude his fast-casual Shake Shack establishments.

[22] EUROPEAN COMM'N, EU DIGITAL COVID CERTIFICATE, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (last visited Sept. 14, 2021).

[23] N.Y. STATE, EXCELSIOR PASS AND EXCELSIOR PASS PLUS, https://covid19vaccine.health.ny.gov/excelsior-pass (last visited Sept. 14, 2021).

[24] Nick Kostov & Eric Sylvers, *France, Italy Require Covid-19 Passes for Restaurants, Bars*, WALL ST. J. (Aug. 10, 2021, 5:34 PM ET), https://www.wsj.com/articles/france-italy-require-health-pass-restaurants-bars-11628587800.

[25] Stuart Winer, *As cases rise, green pass system kicks back in for large events and venues*, TIMES OF ISRAEL (July 29, 2021, 11:24 AM), https://www.timesofisrael.com/green-pass-system-kicks-back-in-for-events-venues-with-over-100-people/.

[26] Aina J. Khan, *Norway lifts coronavirus restrictions after 561 days*, N.Y. TIMES (Sept. 25, 2021), https://www.nytimes.com/2021/09/25/world/norway-ends-covid-restrictions.html.

[27] *See Principles*, Good Health Pass, https://www.goodhealthpass.org/principles (last visited Oct. 5, 2021). In addition, the Linux Foundation Public Health Cardea project is an ecosystem focused on ready to deploy open source code to support interoperable frameworks, which allows frameworks to be more quickly adopted by those who need a system implemented expeditiously. *See Cardea*, Indicio, https://indicio.tech/cardea/ (last visited Nov. 2, 2021).

[28] Concepción de León, *What You Need to Know About Your Vaccine Card*, N.Y. TIMES (June 20, 2021), https://www.nytimes.com/article/vaccine-covid-card.html.

[29] *See* FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT, IF YOU MAKE OR BUY A FAKE COVID-19 VACCINATION RECORD CARD, YOU ENDANGER YOURSELF AND THOSE AROUND YOU, AND YOU ARE BREAKING THE LAW (Mar. 30, 2021), https://www.ic3.gov/media/y2021/psa210330.

[30] *Principles*, Good Health Pass, https://www.goodhealthpass.org/principles (last visited Oct. 5, 2021).

across a number of countries (which may also differ in form or substance) and demonstration of compliance with policy restrictions that also may differ country by country.

These complexities, combined with the imperative of supporting a return to normal in the wake of the COVID-19 pandemic, have reinvigorated conversations about the need to advance existing digital identity systems to support broad and consequential applications like health certificates.

THE DEVELOPMENT OF DIGITAL IDENTITY

While there are no universally accepted definitions regarding digital identity and the lack of common vocabulary often contributes to confusion and ambiguity, for the purposes of illustrating concepts, we will use the following nomenclature in this paper:

- **Attribute:** perty of a person or entity.
- **Claim:** An assertion of attributes made by a person or entity about themselves or another person or entity.
- **Credential:** A digital representation of claims by a holder.
- **Digital Identity:** A digital representation of a person's or entity's attributes. However, the word "identity" itself is a misnomer, as entities such as corporations and Internet of Things devices also have attributes, e.g., a corporation has the attribute of being in good standing to do business in the State of New York. While we will continue to use the term "digital *identity*" in this paper, it may be more accurate to reference a person's or entity's digital status or condition rather than their "identity."
- **Holder:** A person or entity that holds a digital identity about themselves or another person or entity.
- **Issuer:** A person or entity issuing a credential to a holder.
- **User:** An end user of the digital identity ecosystem.
- **Verifier:** The person or entity that is verifying credentials.

The Roots of Digital Identity

To understand how health certificates serve as a catalyst for the advancement of digital identity, it is important to trace the roots of digital identity. The relative nascence of digital identity systems as compared to other Internet technologies is, in part, tied to the history of the Internet itself. In particular, the lack of a digital identity system can be traced back to the early architectural design and implementation of the ARPANET—the precursor to the modern-day Internet.[31] The ARPANET was first developed in the 1960s as a military-funded experiment into networking and packet-switching technology. Given its military and academic origins, the nature and small number of participating institutions, and the unwieldy nature of computers at the time, the need to identify *machines* as opposed to *individuals* was the predominant focus of the early Internet.[32] Reliance on Internet Protocol (IP) addresses that corresponded to a machine on the network, each housed at one of a short list of participating institutions, was sufficient.

To understand how health certificates serve as a catalyst for the advancement of digital identity, it is important to trace the roots of digital identity.

[31] Garrison Breckenridge, *A Brief History of Digital Identity*, MEDIUM (June 4, 2018), https://medium.com/humanizing-the-singularity/a-brief-history-of-digital-identity-9d6a773bf9f5.
[32] *Id.* ("TCP/IP assigns numerical addresses to internet 'hosts' (computers)" rather than to individual users).

Those early design decisions still inform the modern Internet. Today, machines on the network continue to be identified by IP addresses. Information is routed between these machines using the TCP/IP protocol, which uses those IP addresses to determine the location of content or devices on the network.[33] Information on the World Wide Web is further linked using the Domain Name System, which links unique and human-readable domain names to IP addresses and thereby allows users to more easily and reliably access content online. Collectively, these protocols establish a comprehensive system that is still based foremost on identifying machines, but no similarly hardy systems exist for identifying the individuals behind those machines.[34]

PHASES OF ONLINE IDENTITY: THE ROLE OF INTERNET INTERMEDIARIES

Because a comprehensive system of digital identity was not built into the central architecture of the Internet, a host of Internet intermediaries have arisen who are responsible for managing particular aspects of digital identity rather than taking a holistic approach. These intermediaries collect information about Internet users that can be linked to online identifiers such as the IP address of a user's device, cookies stored on that device, or usernames and passwords employed to access particular services. This information includes data personally identifying the user (e.g., name or ID number), assigning them attributes (e.g., their age, sex or gender, residence, and education level), and identifying their preferences (e.g., their online purchase history, websites frequently visited, and what people and brands they interact most closely with online). Depending on the intermediary and the particular use case, such information may be verified or may simply rely on the user or another party's claims about their identity, e.g., through single sign-on technology. However, because today's identity system is primarily controlled by intermediaries (as opposed to individuals themselves) and is largely fractured in structure, the system fails to unlock the full promise of a comprehensive digital identity system.

The evolution of digital identity systems can be classified according to four phases described by Christopher Allen, a specialist in standards and identity who focuses on blockchain technologies.[35] In his article "The Path to Self-Sovereign Identity," Allen posited that, as digital identity systems evolve across these four phases, individuals gain greater control and autonomy with respect to their identities.[36]

- **PHASE 1—CENTRALIZED:** Identities are controlled by a single entity on the basis of information that they have collected about the user, whether directly or through third parties.
- **PHASE 2—FEDERATED:** Individuals can establish an identity with a particular service provider that allows them to log into multiple services.
- **PHASE 3—USER-CENTRIC:** A system of centralized digital identity built with portability and user control at its core.
- **PHASE 4—SELF-SOVEREIGN IDENTITY:** Digital identity is fully controlled by the user and decentralized.[37]

---

[33] Breckenridge, *supra* note 31.

[34] An analog for individual identity is the WHOIS system, which was developed to support the domain name system (DNS). WHOIS identifies and provides contact information for the party who registered a domain name (the "registrant") and other contacts involved in domain management. However, WHOIS does not feature a credentialing authority. Users self-attest their identity and contact information and the provider that handles domain registration (the "registrar") is only responsible for performing basic validations of the format of these contact fields. The registrar does not perform any credentialing to determine that the information contained in the WHOIS output actually belongs to the registrant. *About WHOIS*, INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, https://whois.icann.org/en/about-whois (last visited Sept. 14, 2021).

[35] Christopher Allen, *The Path to Self-Sovereign Identity*, COINDESK (Apr. 26, 2016, 11:02 PM CDT, Updated Sept. 11, 2021, 7:14 AM CDT), https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/.

[36] *Id.*

[37] For a comprehensive discussion of the phases of digital identity and their application to Digital Ledger Technologies, please see Joseph Cutler, J. Dax Hansen & Charlyn Ho, Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues 2, PERKINS COIE LLP (2018), https://www.perkinscoie.com/images/content/2/1/v3/218495/Perkins-Coie-Self-Sovereign-Identity-and-Distributed-Ledger-Tech.pdf.

Today, many digital identity systems are still in Phase 1. In these centralized systems, individual website owners or service providers maintain fragmented profiles about their users (often connected to usernames, which may or may not be based on or related to legal names), based upon information that they have either collected directly or acquired through third parties.[38] This model results in an individual's information being distributed across these various profiles, fragmented, and subject to the control of many masters. The storage of identity-related information across these multiple, incomplete profiles also contributes to the insecurity of data by creating multiple points of failure; if just one of these myriad intermediaries is breached, users could face substantial harm due to the exposure of their personal data.[39] The fragmentation of identity-related information also means that no individual service provider has access to the individual's complete digital identity, impeding users from fully leveraging their digital identities within any single interaction.

Major Internet intermediaries have launched their own versions of federated identity systems (Phase 2) in recent years. For example, individuals can log into many third-party websites and services through either their Facebook profile, Apple ID, or Google account. These federated systems address some of the shortcomings of fully centralized systems. For example, users are afforded greater convenience through the ability to leverage a preexisting digital profile to access a new website or service. They may also gain security benefits because they can entrust their identity information to a single service provider without requiring replication of their personal data.

However, federated systems exacerbate some existing challenges while also introducing new ones. This is due, in part, to the fact that they continue to be managed by centralized intermediaries who are largely motivated by commercial interests. These intermediaries may gain even more power vis-à-vis users through the ability to intermediate their interactions with third-party websites and services. For example, revocation of a credential associated with the service provider managing the central identity credential could leave the Internet user at their mercy, unable to access their other internet profiles and capital or information accumulated or stored therein.[40] And, the federated service provider (rather than the user) may control what aspects of the user's digital identity are shared with these third-party sites, potentially undercutting the user's autonomy over and transparency into how their data is shared.[41] Moreover, if the federated service provider is breached, the user may face even greater harm because other parts of their digital identity may be accessed by way of that central credential. Finally, if a federated service provider goes out of business, is acquired, or otherwise loses control over users credentials, users' can be adversely affected with little to no recourse.

[38] Ana I. Segovia Domingo & Álvaro Martín Enríquez, *Digital Identity: the current state of affairs* 31–36, BBVA RSCH. (Working Paper No. 18/01, 2018), https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf; Christoffer Hernæs, *Who Gets to Own Your Digital Identity?*, TECHCRUNCH (Aug. 22, 2019, 5:00 PM CDT), https://techcrunch.com/2019/08/22/who-gets-to-own-your-digital-identity/.

[39] Segovia Domingo, *supra* note 38, at 31-32.

[40] One facet of this problem is a system operator's ability to manufacture consent and coerce identity-holders into divulging information. ALEX PREUKSCHAT & DRUMMOND REED, SELF-SOVEREIGN IDENTITY § 9.8.3 (2021).

[41] *See* Mary Rundle, *e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector*, OXFORD INTERNET INST., at 12, 14 (Nov. 2007), https://www.oii.ox.ac.uk/archive/downloads/publications/FD12.pdf (arguing that federated systems are overly intrusive with regard to data sharing); *id.* at 19 ("Data treatment that differed from what the user expected would raise questions of fair information practices and data protection. New possibilities for information sharing could lead to new uses of personal data – involving a sort of retro-engineering of the original purpose for which data had been captured (in a legal sense) as data was subject to secondary, or downstream, uses. So, too, with the easy transfer of information enabled by identity systems, service providers might demand identity information that they did not actually need.").

Today, there are no commonly used examples of comprehensive identity systems that are fully user-centric (Phase 3) or self-sovereign (Phase 4).[42] The vision for a user-centric (Phase 3) identity system has motivated a number of efforts to develop identity systems that place greater focus on the user.[43] Unfortunately, however, these attempts fell short because even though people were not under the control of a service, application, or website provider, their digital identities were still managed and controlled primarily by the digital identity service providers and not by the holders themselves.[44] Efforts to develop a self-sovereign digital identity system (Phase 4) are similarly nascent, although developments are underway.[45]

Organizations such as Indicio[46] have observed the deployment of digital identity systems and commented to us that the practical realities of enterprise digital transformation highlight a significant chasm between user-centric (Phase 3) and self-sovereign (Phase 4) systems. Furthermore, adoption of full self-sovereignty may face significant regulatory challenges due to existing privacy and security frameworks that are premised upon traditional, centralized data models and not fully self-sovereign data models, which are disintermediated and (often) decentralized. For example, the authors of the European Union's General Data Protection Regulation (GDPR) began drafting in 2012—a period in which centralized data models proved the norm. Such models often required that users create online accounts to interact with third-party intermediaries who, in turn, exercise control over such users' data. Centralized models heavily influenced the thinking of the drafters of the GDPR, which is one reason the GDPR categorizes entities into "data subjects" (i.e., the users) and "data controllers" of data subjects' data. In a truly self-sovereign ecosystem, data subjects could be their own controllers and therefore the two roles could be collapsed under the GDPR.

Today, there are no commonly used examples of comprehensive identity systems that are fully user-centric

Therefore, Indicio posits that between Phases 3 and 4 exists an intermediate phase which it refers to as "decentralized identity," and which we will call Phase 3.5. Under a decentralized identity model, decision-making and control over users' digital identity is not concentrated with a central entity; rather, the collection, storage, and other processing of data is distributed across the digital identity ecosystem. Furthermore, the decentralized identity model—like the user-centric model—puts user centricity at its core and empowers users to choose with whom they share their data and for what purposes by engaging in peer-to-peer transactions largely without intermediaries. However, unlike in a truly self-sovereign model, in a Phase 3.5 model verifiers can dictate data governance agreements with users regarding how the data will be used and may even override an individual's decision about their data with sufficient cause.[47] For example, in Indicio's partnership with SITA (the leading global provider of technology to the air transport industry) and the island of Aruba's Department of Public Health,[48] users must, at

[42] *See* Allen, *supra* note 35.
[43] *See* FIDO ALLIANCE, https://fidoalliance.org/; https://www.varonis.com/blog/what-is-oauth/; Rob Sobers, *What is Oauth? Definition and How it Works*, VARONIS INSIDEOUT SECURITY BLOG, https://auth0.com/docs/protocols/openid-connect-protocol.
[44] *See* Marcos Allende López, *Self-Sovereign Identity The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain* 15, 17, INTER-AM. DEV. BANK (2020), https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.
[45] For more information on one such proposed identity system, please see the Sovrin Foundation's white paper, "The Inevitable Rise of Self-Sovereign Identity," available at https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.
[46] *Who We Are*, Indicio, https://indicio.tech/about/ (last visited Oct. 25, 2021).
[47] *Cf.* Heather Dahl, *Digital credentials and privacy in the time of COVID-19*, OECD (Nov. 13, 2020), https://oecdonthelevel.com/2020/11/13/digital-credentials-and-privacy-in-the-time-of-covid-19/.
[48] *Island of Aruba trials open source SITA COVID health credential solution*, Ledger Insights (May 10, 2021), https://www.ledgerinsights.com/island-of-aruba-trials-open-source-sita-covid-health-credential-solution/.

present, wait a significant period of time before withdrawing their COVID-19 health credential from Aruba's health department. This waiting period ensures sufficient time for the department to make public health decisions, compile a regulatory archive, and meet auditing requirements, as opposed to vesting full and complete control in the users, themselves.

Applying Phases to Health Certificates

Despite the winding trajectory of digital identity development, recent discussions related to health certificates have brought public attention back to the need to identify a workable digital identity solution, as well as the challenges that plague existing systems.[49] Given the significant physical and emotional health risks and correlating financial impacts associated with transmission of the coronavirus on both individualized and community scales, it is important that a system accurately captures an individual's vaccination or testing status in real time.[50] Mere self-attestation, which may be adequate to support other low-risk activities, may not be sufficient when public health is on the line.

Additionally, a system of health certificates could, ideally, support a diverse range of interactions that were disrupted by the pandemic—everything from international and domestic travel to in-person employment within both "essential" and "nonessential" sectors to recreational activities.[51] The cross-contextual need for health certificates reveals the weakness of fragmented identity systems. Ideally, individuals should be able to establish their identity once and leverage it across these relevant purposes and systems, rather than having to undertake the potentially tedious (and, from a privacy perspective, risky) process of attesting to their identity and undergoing credentialing for each possible interaction or even repeatedly for a singular interaction. It is also important to acknowledge the fundamental nature of these activities—employment, mobility, and education, for example—which highlights the need to streamline sharing of this information and allow enhanced user control. As such, the risks associated with entrusting management of a comprehensive digital identity system to any single intermediary, especially one that is commercially motivated, are particularly acute.

Finally, it is also important to consider the nature of data that would be contained within the system, to determine effective steps for incentivizing users to populate the system with information about their identity. Higher-risk data will need to be met with similarly high standards for protection of data privacy and security, as well as selective data disclosures, in order for users to embrace such systems, provide value, and create an incentive for expanding their data profiles.

Many of these user-centric principles—such as users' right to correct or delete their personal data (subject to certain exceptions), ensure transparency concerning how their personal data is used and shared, or apply reasonable security measures to their data—are already enshrined in many privacy laws like the California Consumer Protection Act and the EU's GDPR referenced above. However, regardless of whether laws mandate honoring such user rights and protections, we propose that such attributes are essential pillars to creating a digital identity system that engenders trust and widespread adoption.

[49] *See* Kumanan Wilson & Colleen M. Flood, *Implementing digital passports for SARS-CoV-2 immunization in Canada*, 193 CAN. MED. ASSOC. J. E486, E486–87 (Apr. 6, 2021), https://www.cmaj.ca/content/193/14/E486; Katya Pivcevic, *Immunity Passports Face Familiar Digital Identity Challenges on Interoperability, Privacy*, BIOMETRICUPDATE.COM (Feb. 8, 2021), https://www.biometricupdate.com/202102/immunity-passports-face-familiar-digital-identity-challenges-on-interoperability-privacy.

[50] *See, e.g.*, Cardea, https://cardea.app/ (last visited Oct. 5, 2021).

[51] Dan Diamond, Lena Sun & Isaac Stanley-Becker, *'Health passports' Are on the Way, but Developing Them Won't Be Easy*, WASH. POST (Mar. 28, 2021, 11:00 AM EDT), https://www.washingtonpost.com/health/2021/03/28/vaccine-passports-for-work/.

Considering the foregoing, it is clear that most pre-pandemic digital identity systems are inadequate to meet the challenge. To procure sufficient buy-in from holders and verifiers alike, a health certificate system should possess many of the characteristics of a user-centric (Phase 3) model and, ideally, a decentralized (Phase 3.5) model.

In particular, it is imperative that any health certificate system instill trust in the accuracy of its data, provide user-centricity and autonomy in establishing and using one's digital identity, and feature robust data privacy and security protections.

VALUES OF DIGITAL IDENTITY

Identity is a core aspect of personhood, playing a significant role in how one interacts with and is recognized by society, which is equally salient in the context of digital identity.[52] While some interactions rely heavily on one's identity (e.g., providing individualized healthcare), others require only superficial identification (e.g., a simple in-store purchase or loyalty program). In an increasingly digital environment, where individuals may opt for telehealth treatment or purchase items in a digital marketplace, digital identity is an essential part of personal identity.[53] While online, individuals must still be able to identify themselves and attest to attributes about themselves to meaningfully engage with such services in the same way they do in the physical world.

However, the physical identification cards that are often used in the offline world may fall short in these online contexts.[54] Identification cards may be of little value if photo identification or other security features cannot be used in an online context; or, they may not contain all of the information to which the user desires or is required to attest. Conversely, physical identification cards may contain much more information than the user wishes to share or needs to share to participate in an online context.

Digital identity systems should be able to provide similar (or greater) assurances to their physical counterparts.[55] As noted at the outset of this paper, in order to ensure that digital identity systems are embraced by both individual holders and verifiers, a comprehensive digital identity system must emphasize three pillars: 1) trust that a digital identity is what it purports to be; 2) user-centricity, based upon an individual's ability to exercise control over their digital identity; and 3) data privacy and security. Each is addressed in turn below.

[52] "Stated simply, when individuals are not in effective control of identity information, personhood and the enjoyment of human rights shrink. . . . In other words, the danger is that what is relevant is no longer *personhood* – the recognition of a person as having status as a person – but rather a *profile* – the recognition of a pattern of past behaviour. Those past actions themselves are not the source from which his human rights derive; rather, the state of being a person gives rise to those rights." *At a Crossroads: "Personhood" and Digital Identity in the Information Society* (OECD, Sci, Tech., & Indus., Working Paper No. 2007/7, Feb. 29, 2008), https://www.oecd.org/sti/ieconomy/40204773.doc.

[53] *See* CHARLYN HO, DOMINIQUE SHELTON LEIPZIG, ARSEN KOURINIAN & STEPHANIE SALADINO, FROM TELEMEDICINE TO VIRTUAL CARE: DATA PRIVACY AND OTHER LEGAL ISSUES SURROUNDING VIRTUAL HEALTH IN THE POST-COVID WORLD, PERKINS COIE, MICROSOFT (May 19, 2021) (on file with authors). This white paper is the product of a joint collaboration between Perkins Coie LLP and Microsoft Corp.

[54] R. JESSE MCWATERS, WORLD ECON. FORUM, A BLUEPRINT FOR DIGITAL IDENTITY THE ROLE OF FINANCIAL INSTITUTIONS IN BUILDING DIGITAL IDENTITY at 17-18 (Aug. 2016) (discussing the trends that portend increased adoption of digital identity systems), http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[55] *See* PREUKSCHAT, *supra* note 40, at § 9.

TRUST

An identity system is of little value if parties cannot rely on the validity of its contents. To be useful to verifiers, a system needs to establish that the identity information and related attributes held by the system are, in fact, authentic to what the holder attests.[56] Like trust in human relationships, this ability to rely on the accuracy or veracity of a digital identity is what we refer to as "trust." However, establishing "trust" in a digital world can be a very different process than forging trust in human relationships, given the fact that interactions over the Internet are not conducted face-to-face and can even be anonymous. Trust in the digital world can be established in a number of ways, including through a verification process carried out by an authority with the ability to confirm the truth of the individual's identity claims.[57] These can be the same authorities used in offline contexts (such as governmental agencies) or new ones, provided that they are able to establish the requisite reliability through confirmation of the validity of attested identity attributes. Trust allows digital identity to be used cross-contextually without each party that relies on the digital identity system having to reestablish the truth of its contents.[58]

An identity system is of little value if parties cannot rely on the validity of its contents.

Physical driver's licenses issued by state departments of motor vehicles (DMVs) are one of the most common examples of a physical identity credential (in large part due to their tamper-resistance) and corresponding trusted credentialing authority.[59] These driver's licenses are used in numerous offline contexts to convey a range of attributes (e.g., identity, age, home address, and licensure). The ability of these identity verifiers to rely upon physical driver's licenses for a range of important purposes, such as opening financial accounts, operating a motor vehicle, and traveling to a foreign country, is based upon trust instilled in the DMVs as issuers to accurately reflect individuals' identities and attributes, as well as features that help ensure that the physical card is authentic and properly belongs to the individual.[60] However, physical identity cards may also divulge more information than the holder would like to provide (or the verifier would like to accept). A driver's license, for example, may display a holder's image, name, date of birth, address, sex, eye color, donor status, state of issuance, signature, and license number—not all of which may be necessary or appropriate to share in a given context.[61]

The information on physical identity credentials may be more easily falsified, potentially requiring additional safeguards when it comes to verification, when used with digital or online vendors. For example, a vendor could swipe, handle, and observe physical attributes (such as a hologram) of a driver's license to ascertain its authenticity, but a virtual vendor may rely only on a picture of the driver's license—a medium less directly tied to the originally

---

[56] *See generally* CLARE SULLIVAN, DIGITAL IDENTITY (Univ. of Adelaide Press 2000) (discussing data verification in the United Kingdom); U.S. AGENCY FOR INT'L DEV., IDENTITY IN A DIGITAL AGE: INFRASTRUCTURE FOR INCLUSIVE DEVELOPMENT 2, 4 (2017), https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf. ("Identification is ultimately about trust."); Segovia Domingo, *supra* note 38, at 18 ("Digital identity is a way for an individual or a business to prove who they are online with a certain level of trust."); Axel Domeyer et al., *How governments can deliver on the promise of digital ID*, MCKINSEY & CO.: PUB. & SOC. SECTOR (Aug. 31, 2020), https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id.

[57] For example, driver's licenses and birth certificates in the United States are issued by various state agencies and departments.

[58] *See* Segovia Domingo, *supra* note 38, at 21; MILES CHEETHAM, PIRAN PARTNERS, DIGITAL IDENTITY: THE COMMERCIAL OPPORTUNITY § 7.1 (Dec. 2013), http://piranpartners.com/wp-content/uploads/2014/12/Digital-Identity-The-Commercial-Opportunity.pdf. ("A Digital Identity can deliver better accountability in transactions as it creates a bond of trust between the individual and the online service or resource.").

[59] *See* MCWATERS, *supra* note 54, at 69.

[60] *See* SULLIVAN, *supra* note 56, at 39 n.95 ("This is true for authentication on registration as well for verification at the time of a transaction because the individual establishes his or her identity by producing documents such as birth certificate, driver's license, credit cards and other government-issued cards. The information in these documents is cross-checked to see if it matches and, where possible, it is checked against the database of the relevant department/agency.").

[61] *See Decentralized Identity & Healthcare, Part 1 The Importance of Strong Governance* 12, LUMEDIC (Nov. 10, 2020) https://dzrxzp7tgg4x3.cloudfront.net/documents/Lumedic-Paper-Pt1-v3_2020-11-10-223625.pdf?mtime=20201110143625&focal=none.

issued credential and in which some of its original security mechanisms could be rendered void (such as the feel or size of the ID card or any embedded holographic imaging).[62]

To be useful, digital identity systems must be able to establish trust similar to that vested in the governmental agencies—providing confidence that the holder's purported identity claims are, indeed, true. This depends upon the credential's ability both to accurately reflect the attributes of the holder and to provide assurances that the credential is being used by the person to whom it was assigned. Given such weaknesses when certain traditional physical identifiers are used in new, digital realms, some new intermediaries have arisen that help transfer these identifiers from offline to online. For example, Jumio has built a solution that attempts to better leverage the value of offline identifiers in online contexts that require higher trust, such as banking or industries with Know Your Customer (KYC) requirements.[63] Users submit a photo of a physical identifier, along with a contemporaneous "selfie" of themselves, that is quickly analyzed in the verification process through the use of facial recognition technology to help ensure that the user is who they purport to be.[64] While these types of solutions provide greater trust in verification, they fall short of establishing the type of universally recognized trust required for cross-functional and multi-contextual application of a digital identity system.

The need for trust is at the heart of the ongoing public discourse about health certificates.

The need for trust is at the heart of the ongoing public discourse about health certificates. Because the United States has not moved forward with a health certificate system at the national level,[65] as various in-person activities resume, requirements that participating individuals are vaccinated (or otherwise demonstrably COVID-negative) are most often based upon self-identification without any related credentialing.[66] However, between the trend of vaccine hesitancy and examples of some individuals forging vaccination certificates,[67] such trust cannot be readily established. Incidents of paper vaccination card fraud are on the rise, and validating the information on a paper vaccination card is not easy or—in many cases—even an option for employers, medical facilities, and commercial establishments.[68] Even if validation and authentication were possible, the time and expense may not be practical for many commercial establishments and small business enterprises.

If properly implemented, health certificates can help bridge this gap by providing a widely usable basis for not only self-identifying as to one's vaccination status, but *actually verifying* such status.

---

[62] *See* Sadek Ferdous, Farida Chowdhury & Madini Alassafi, *In Search of Self-Sovereign Identity Leveraging Blockchain Technology*, 7 IEEE ACCESS 103059, 103074 (July 25, 2019) ("An offline verification process might require Alice to provide a physical document (e.g. passport, identity card and so on) as a claim regarding the citizenship/residency of Alice for that particular country to a registration center. On the other hand, an online verification might involve uploading the scanned cop[y] of the required physical document to an online service which then can be verified either via an advanced image analysis mechanism or via human inspections.").

[63] *Jumio ID Verification*, JUMIO, https://www.jumio.com/products/id-verification/ (last visited Sept. 14, 2021).

[64] *Id.*

[65] Arijeta Lajka, *The U.S. government has no plans to require 'health passports'*, AP NEWS (Apr. 6, 2021), https://apnews.com/article/fact-checking-afs:Content:10051817171.

[66] Elliott Davis, *These States Have Banned Vaccine Passports*, U.S.NEWS & WORLD REP. (June 1, 2021, 3:13 PM), https://www.usnews.com/news/best-states/articles/which-states-have-banned-vaccine-passports.

[67] Kevin Collier & Ben Collins, *Pro-Trump web forums are abuzz with directions to forge Covid vaccine cards*, NBC NEWS (Apr. 29, 2021, 6:06 PM CDT), https://www.nbcnews.com/tech/tech-news/covid-vaccination-card-fraud-prompts-cdc-action-rcna802.

[68] *See* Davis, *supra* note 66.

USER-CENTRICITY

A user-centric system grants the holder primary power and control in establishing their digital identity and attesting to their attributes.[69] Individuals should also retain the ability to control how their digital identity and related attributes are used, including determining the parties to which they are revealed and for what purposes.

The consequences faced by those who are left out of centralized identity systems help demonstrate the benefits of user-centricity and autonomy in the development of a digital identity system. Today's offline identification systems are not fully inclusive. USAID estimates that roughly 1.1 billion people are wholly excluded from national ID systems, potentially leaving them "invisible, discounted, or left behind" when it comes to services that rely on such identity verification.[70] Others may be included within such systems, but have their attributes incompletely or improperly specified therein. For example, foreign nationals may face difficulties demonstrating their educational or professional credentials within the systems of another country.[71]

A digital identity system focused on user-centricity would help address this by vesting the power to make claims and share credentials of such claims with the holders themselves, rather than placing such power with a centralized entity.[72] If global in scope, such a system could help over a billion displaced persons more seamlessly reclaim their identities and integrate the social reputations and intellectual capital developed in their home nations into their present lives. Moreover, with universal buy-in, employers, educators, medical service providers, and other sources of identification validation could more seamlessly assist in establishing or authenticating digital identities.

The benefits of user-centricity may also encompass how holders share their information.[73] The example of the physical driver's license demonstrates some of the weaknesses of offline identity systems when it comes to controlling how one's identity credentials are shared.[74] Driver's licenses serve different functions in different contexts. In some, they are used to validate the individual's identity (e.g., when voting or opening a bank account). In others, they are used to establish a holder's attributes where knowledge of their actual identity may or may not be essential (e.g., whether they are of legal drinking age or properly licensed to drive). However, even in contexts where knowledge of the individual's actual identity is not necessary, the holder is nevertheless required to share all information reflected on the license in order to attest to the particular attribute.[75]

Digital identity systems possess a potential advantage over physical cards because the holder may choose to share only the information that is needed to fulfill a particular purpose. For example, KYC requirements may require a service provider to verify certain attributes about its business customers for risk assessment purposes.[76] A user-centric digital identity system could allow such customers to reliably attest to the relevant information about their

---

[69] *See* Segovia Domingo, *supra* note 38, at 35.
[70] IDENTITY IN A DIGITAL AGE, *supra* note 56, at 1.
[71] *See, e.g.*, Joey Peters, *Highly trained and educated, some foreign-born doctors still can't practice medicine in the US*, PUB. RADIO INT'L: THE WORLD (Mar. 28, 2018, 9:00 AM EDT), https://www.pri.org/stories/2018-03-26/highly-trained-and-educated-some-foreign-born-doctors-still-can-t-practice.
[72] *See* Kim Cameron, *The Laws of Identity*, MICROSOFT CORP. (May 11, 2005), http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (positing a 7-rule model for user-centric identity management); *see also* JOHN VACCA, MANAGING INFORMATION SECURITY at 81–82 (2d ed. 2013).
[73] *See* VACCA, *supra* note 72, at 90; LUMEDIC, DECENTRALIZED IDENTITY & HEALTHCARE, PART 2, PATIENT CENTRICITY FULFILLS HIPAA 5 ("[I]nformation sharing issues can be addressed by fundamentally shifting the patterns of data exchange in healthcare to focus on the *individual* as the source and steward of their own data.").
[74] *See supra* notes 59–62.
[75] *See supra* note 62.
[76] Djuri Baars, *Towards Self-Sovereign Identity Using Blockchain Technology* 36–39, UNIV. OF TWENTE (2017) (discussing KYC attribute sharing in the context of customer onboarding).

businesses (e.g., years of operation, possession of relevant licenses) without sharing documentation that could reveal unnecessary personal information about the company's owners or employees.[77]

To be effective, the information contained within a health certificate system would necessarily contain personal information. These systems would need to not only identify individuals but also include personal health information about those individuals, such as their vaccination status, testing results, or information about confirmed COVID-19 cases. Given the potentially sensitive nature of this data, individuals would likely be unwilling to participate in a health certificate system if doing so meant surrendering all control of this information to a third party.[78] Accordingly, to be widely embraced by users, a health certificate system should vest the primary power to determine whether to share, how to share, and how to use credentials to the credential holders themselves, as well as allow those individuals to control how that information is shared.

The potential scale and cross-jurisdictional nature of a comprehensive health certificate system, which could be used for many diverse use cases and across jurisdictions worldwide, also underscores the value of user-centricity in such systems.

User-centricity helps address issues related to diversity and scale by making holders themselves responsible for the central process of attesting to their identity and triggering the relevant confirmation processes,[79] and by enabling verifiers to confirm these claims as needed based upon the information provided.[80] A system should be similarly user-centric with respect to how information is shared for verification purposes. For example, an individual may reasonably decide that based upon their importance and the safeguards in place, certain contexts (like their employment) warrant sharing the personal information contained within a health certificate system, while others (like dining out) do not. Entrusting these important decisions to a third party could have a chilling effect on users' overall embrace of a health certificate system.

User-centricity helps address issues related to diversity and scale by making holders themselves responsible for the central process of attesting to their identity and triggering the relevant confirmation processes, and by enabling verifiers to confirm these claims as needed based upon the information provided.

PRIVACY AND SECURITY

As evidenced by the rising costs associated with high-profile ransomware attacks[81] and other data and security breaches,[82] providing adequate data protection is more critical than ever in digital contexts. Nowhere is this more true than in the context of digital identity systems that fundamentally depend upon the users of such systems sharing and storing information about their identity.[83] Users could face harm if such information was breached, whether due to accident or purposeful attack. Further, even if information is not breached, users could face hardships if certain personal information was shared or used for purposes they were unaware of or had no control over. For these

[77] *Id.*
[78] *See* Auxier et al., *infra* note 93.
[79] *See Ontario's Digital ID: Technology and Standards*, ONTARIO, https://www.ontario.ca/page/ontarios-digital-id-technology-and-standards (last visited Sept. 16, 2021) (articulating a framework by which users possess control over how information is shared, with whom, and how much).
[80] *See id.*
[81] *See, e.g.*, Brian Fung, *Colonial Pipeline says ransomware attack also led to personal information being stolen*, CNN BUSINESS (Aug. 16, 2021, 1:10 PM ET), https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.
[82] Steve Alder, *The Average Cost of a Healthcare Data Breach Is Now $9.42 Million*, HIPAA J. (July 29, 2021), https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/.
[83] *See generally* HO ET AL., *supra* note 53 (discussing the sharing of sensitive information in the context of virtual healthcare).

reasons, it is essential that any digital identity systems feature robust privacy and security protections to give users the confidence to populate such systems with their personal data, knowing that it will be kept private and secure.

The ability to more precisely control what information is shared in a user-centric digital identity system also functions as a privacy feature. Data minimization requirements and purpose-based processing feature at the core of many global privacy laws.[84] However, these principles are in tension with physical credentials, which, depending on their particular design, may require that holders share more information about themselves than is required for a particular purpose.[85] In addition, where such information is kept by verifiers, the holder may lack visibility into and control over correction of inaccurate or incomplete data, data retention terms, and any onward sharing of that information.[86]

A digital identity system has the potential to be more privacy-protective by allowing the holder to limit the sharing of their information to that which is strictly necessary for a particular purpose…

In addition to reducing users' control over the sharing of their information, this feature of physical identity systems also introduces risks, because greater sharing of information expands the surface area for potential breach or other misuse of their information. A digital identity system has the potential to be more privacy-protective by allowing the holder to limit the sharing of their information to that which is strictly necessary for a particular purpose and by providing greater visibility into how data is retained and shared.[87] For example, when a user creates an account to access online services, they provide the online service provider with personal details that the online service provider can retain and use. However, if the system is appropriately designed and privacy-preserving, a holder can choose to share digital credentials for the sole purpose of credential verification and can likewise choose to fully revoke access to such information at their discretion (excluding data strictly necessary for a verifier to fulfill its own regulatory compliance obligations).

Technical security mechanisms also come into play. For example, the encryption of data when it is both in transit and at rest can significantly reduce the risks associated with a potential breach, by rendering data unreadable by anyone other than the intended recipient.[88] Similarly, multi-factor authentication requires that an individual provide multiple proof points before gaining access to a system, generally by supplying both something they know (such as a password) and something they have (such as a physical device or token that has been assigned to them).[89] Multi-factor authentication dramatically reduces the risks associated with phishing attacks and other threats to one's digital identity, as compared to systems that rely on

[84] *See* Gen. Data Prot. Regul. 2016/679, art. 5, Principles relating to processing of personal data, https://gdpr-info.eu/art-5-gdpr/; Brazilian Data Prot. Law (LGPD) art. 6, https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.
[85] *See, e.g.*, LUMEDIC, *supra* note 61, at 12.
[86] *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom* 29, ACLU (May 17, 2021), https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf ("While digital IDs have some advantages for Holders, such as selective data disclosure, a physical document is concrete, can't be quickly or easily modified, and stays under the control of the person who possesses it.").
[87] *Id.* at 17.
[88] *See, e.g.*, Joanna Stern, *Wallets Are Over. Your Phone Is Your Everything Now.*, WALL ST. J. (Updated Sept. 5, 2021, 6:26 PM ET), https://www.wsj.com/articles/wallets-are-over-your-phone-is-your-everything-now-11630846800?st=q8trmtqz6i30oiz&reflink=article_email_share ("Apple says the system is built so you don't need to hand over your phone to anyone—or even unlock it. Customers' identity data is encrypted, and Apple and the issuing states don't know when or where you present your ID, Apple says. . . . Any card I drop on the street—or even hand over in a restaurant—could be abused by any unscrupulous character. On a secure device, with my info encrypted and biometrically protected, that's much harder.").
[89] *See generally* Charlie Jacomme & Steve Kremer, *An Extensive Formal Analysis of Multi-factor Authentication Protocols*, 2018 IEEE 31ST COMPUT. SEC. FOUNDS. SYMP. (July 2018), https://ieeexplore.ieee.org/document/8429292 (discussing the applicability of multi-factor authentication protocols).

password protection alone.[90] In light of recent breaches involving several government systems and networks that were presumed to be highly secure,[91] security efforts have emphasized the value of zero trust systems.[92] Zero trust systems presume that no individual is inherently trustworthy, even if they are able to gain access to a protected network.[93] Instead, such systems determine trustworthiness for the purpose of access through a range of factors (such as network location, device status, credentialing, behavioral information, and more) that collectively determine whether a user is likely to be who they purport to be and grant access accordingly.

The growing volume, scale, and publicity of data breaches[94] has made users more conscious of the security risks associated with sharing their information, particularly in digital contexts.[95] Individuals who believe their data is unsecure or can be easily re-correlated to them after an attempted revocation will likely be unwilling to share their personal information. However, the success of a comprehensive digital identity system necessarily depends on users' willingness to do just that. Security mechanisms like encryption, multi-factor authentication, and zero trust can help bridge that gap by enabling information sharing and verification without the security risks associated with storing the very details contained within the proof.

The sensitive nature of the data that would populate a health certificate system also underscores the need to build adequate data privacy and security protections into the underlying design of a digital identity system. Many jurisdictions that have developed comprehensive privacy legislation recognize that protected health information (PHI) of this nature is among the categories of sensitive personal data to which heightened protections or stricter processing restrictions may apply. The Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, is but one well-known U.S. regulation that defines protected health information, regulates its use and disclosure, and establishes privacy and security standards for covered entities[96] and their business associates[97] or other third parties with which protected health information, or PHI, is shared.[98] Studies show that

---

[90] Microsoft & Chubb, *Email: Is the Digital Door Propped Open for Identity Hijackers? Multi-Factor Authentication Helps Shut Cyber Criminals Out* 8–9 (2020), https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/cyber-insights/documents/pdf/2020-12.10%2017-01-0279%20MFA%20Helps%20Shut%20Cyber%20Criminals%20Out.pdf.

[91] *See* Fung, *supra* note 79 (discussing the Colonial Pipeline ransomware attack that significantly impaired gasoline distribution across the Eastern United States).

[92] *See generally* Sudakshina Mandal, Danish Ali Khan & Sarika Jain, *Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic*, NEW GENERATION COMPUTING (June 2021), https://www.researchgate.net/publication/352824713_Cloud-Based_Zero_Trust_Access_Control_Policy_An_Approach_to_Support_Work-From-Home_Driven_by_COVID-19_Pandemic (describing how zero trust solutions are used to create new access control policies).

[93] *Id.*, at 3 ("The fundamental concept of zero trust is 'never trust, always verify'.").

[94] "Despite 1,923 breaches (49%) without a confirmed number of records exposed, the total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year since we have been reporting on data breach activity." Daniel Lohrmann, *2020 Data Breaches Point to Cybersecurity Trends for 2021*, GOV'T TECH: LOHRMANN ON CYBERSECURITY (Jan. 22, 2021), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html.

[95] *See generally* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (studying U.S. citizens' opinions on data sharing across various contexts).

[96] Covered entities include healthcare providers, health plans, or healthcare clearinghouses that transmit health data electronically for transactions regarding which the U.S. Department of Health and Human Services has adopted standards.

[97] A business associate is an organization or individual who performs services on behalf of a HIPAA-covered entity that requires access to, or the use of, protected health information.

[98] 45 C.F.R. § 160.103 and 45 C.F.R. § 164(A), (E). "Protected Health Information" relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. *Id*. An individual's COVID-19 vaccination status would be PHI and covered by HIPAA's Privacy Rule and Security Rule, but the use and disclosure of this information is only protected with respect to covered entities and business associates, not to other entities such as an individual's employer, a restaurant, airline or other common carrier, hotel, college or university, athletic stadium, etc. There are myriad federal and state employment laws that would potentially be implicated regarding an employer's right to use and disclose an individual's vaccination status beyond the scope of this paper. However, the Equal Employment Opportunity Commission has already opined that it is permissible for an employer to require proof of COVID-19 vaccination of its employees under certain circumstances without running afoul of the

such health-related information may face particular risks when it comes to data security. A report on data breaches in the healthcare sector observed 3,705 healthcare data breaches of 500 records or more.[99] It further noted that those breaches have "resulted in the loss, theft, exposure, or impermissible disclosure of 268,189,693 healthcare records," equating "to more than 81.72% of the population of the United States."[100]

Sensitivities related to the sharing of such data have contributed to the hesitancy around adopting a system of health certificates in certain contexts. A robust system of privacy and data protection would contribute to the success of a health certificate system by helping to instill confidence in holders that they could store health-related records within the system without fear of breach or misuse of the data.

CONCLUSION

Digital identity systems are here to stay. In light of COVID-19's continued resilience and the increasing calls for strong proof-of-vaccine measures, health certificates may prove to be the catalyst that pushes the United States toward a more comprehensive digital identity regime and ignites the spark that brings economies across the globe back to life. But regardless of their origins, digital identity systems will have little success gaining public confidence and widespread acceptance unless they are designed with, at a minimum, the three pillars of trust, user-centricity, and data privacy and security in mind. Such systems, especially those operating in a space as sensitive and salient as vaccination and testing status, must engender public trust that users' data will be secured and users' privacy respected. They should enable testing centers to swiftly provide accurate user data upon request—and only to the true data subject. They should minimize who has access to stored data and who may manage such data. And they should be developed upon architecture that is tamper-proof and incapable of fraud. Without these guardrails, there is little hope that any digital identity system could earn the trust of a COVID-weary citizenry already wary of "big data."

In sum, without a commitment to the three digital identity pillars, we risk stumbling into health credential systems that merely work well enough, rather than committing to restoring people—and their choices—to the heart of the digital identity dialogue. A user-first approach can help avoid the friction that many health credentials have created and lead to a full economic recovery.

Americans with Disabilities Act or the Genetic Information Nondiscrimination Act. U.S. EQUAL EMP. OPPORTUNITY COMM'N, *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[99] *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Oct. 25, 2021).

[100] *Id.*