20

VERIFICATION THEATRE AT BORDERS AND IN POCKETS

Michael Veale

20.1 Introduction

The COVID-19 pandemic saw individuals asked to prove health-related characteristics in a wide and varying array of situations. These differed across jurisdictions. Some countries imposed requirements in occupational and leisure situations. Others made little use of proof mechanisms, or left their use up to private actors. Internationally, however, the idea of 'vaccination passports' co-evolved with legal requirements to prove health-related characteristics *at the border*. This in turn placed domestic pressure on countries to either publicly provide or facilitate private provision of technical infrastructures that could meet emerging international standards of proof.

Before the COVID-19 pandemic, the most similar provision at borders was in relation to yellow fever. Requirements for travelers to have yellow fever vaccinations are typically imposed by countries without the virus but vulnerable to its establishment due to mosquito vectors and non-human primate hosts.[1] The International Certificate of Vaccination or Revaccination against Yellow Fever was replaced from 2007 by the more general International Certificate of Vaccination or Prophylaxis (ICVP).[2] Although the WHO describes ICVP paper certificates—often known as a yellow card, or *carte jaune*—as 'easily lost and prone to fraud',[3] use of these rarely if ever required 'proofs of the veracity of the document'.[4] This is despite significant evidence of forgery. In a recent study, two-thirds of the ICVPs from travelers interviewed at a Sudanese airport appeared to be counterfeit.[5] In these contexts, this could be considered a minimum, as features of the ICVP make it impossible to truly validate. These issues are compounded by challenges further up the supply chain such as vaccine falsification.[6]

DOI: 10.4324/9781003394006-27

This chapter has been made available under a CC-BY-NC-ND 4.0 license.

Contrary to the ICVP, discussions of COVID-19 documentation had functionalities related to proof built into them from the start. European guidelines focused on verifiability as a key design criterion.[7] Several jurisdictions where the ICVP are used as the official record and 'source of truth' of COVID-19 vaccinations later removed their admissibility as proof in day-to-day circumstances.[8] This makes it important to consider what verifiability could and in practice does mean in these contexts.

20.2 Verifiability Theatre

We often verify our identities or verify we possess certain attributes. Verification of a characteristic of an individual is conceptually a two-step process. The first step is authentication of identity—linking the person in front of you to an identifier. The second step is the linkage of that identifier to a characteristic, such as vaccination, testing or recovery. This process further requires integrity of the data involved in this process.

It is worth considering what 'digital' means in this context. Digital is often thought of as an app or a website versus a paper document. This is an important distinction when considering a 'digital divide'; even in a country with high technology saturation such as the UK, 7% of individuals still lack a device which can connect to the Internet.[9] However, even a paper certificate with a QR code is 'digital' insofar as it relies on a 'stack' of infrastructure to generate, maintain, authenticate and interact with it. It is simply the case that the role of the individual in the digital infrastructure is only to obtain and display information—the 'intelligence' happens elsewhere in the network.[10]

20.2.1 Only as Strong as the Weakest Link

In practice, the deployed digital verifiability strategies provided little defence against moderately determined fraud.

Some countries recorded initial vaccinations on paper vaccination cards, such as the United States from the CDC or in the *carte jaune* in Germany. In the United States, these were accepted as proof directly. In Germany, these were both broadly directly accepted as proof, as well as used a source of truth, without reference to other databases, to convert them into digitally signed certificates by most pharmacies.[11]

Hand-signed paper vaccination cards are typically trivially forged. In a poll commissioned by *The Economist*, 12% of American adults under 30 admit knowing somebody with a fake US vaccination card.[12] Thousands of cases of forged *cartes jaunes* are subject to investigation and prosecution procedures in Germany.[13] Those prosecuted included high-profile celebrities, including football coaches.[14] Forgeries of such cards are commonplace concerning yellow fever vaccination in sub-Saharan Africa.[15]

Paper cards with no in-built mechanism of digital linkage of an identifier to a vaccination status were widely accepted around the world despite no practical method of verifying them. The Washington State Department of Health verification guidance illustrates this, with guidance to 'be suspicious of cards printed on thin paper or edges that appear cut by scissors'; to check all fields are completed and the template is the expected one; and to look up vaccine lot numbers to check if such a lot was ever distributed. CDC passes were not printed on secure paper (as ballot papers sometimes are), and so such paper is easily emulated. The latter check is easily passed by copying a valid vaccination batch-time combination from any other card.

Despite this, and seemingly for political reasons, US vaccination cards were accepted around the world as proof at borders and often within domestic regimes and in line with restrictions placed there.

In Germany, the situation was in some ways worse. As with many countries lacking health informatics, the *carte jaune* was used as the source of truth to populate the cryptographically assured digital vaccination pass database. Individuals would walk into pharmacies, who would examine evidence and enter it into a database. At this point, fraudulent *cartes jaunes* could effectively be laundered into a real vaccination pass. This author, holder of a valid UK vaccination record, presented the UK documents to a pharmacist in Berlin in 2021, who looked at the printout without seeking to validate the UK QR code (which at the time was not able to be validated with a German validator, a situation which later changed), and entered the record into the German database, issuing a German vaccination certificate.[16] Indeed, pharmacies in Germany stated they would transform CDC cards and other unverifiable and easily forged foreign vaccination records into German digital certificates.[17]

Fooling pharmacists was not even necessary for those forging at scale, who set up fake pharmacies in order to create irrevocable certificates in Germany. An investigation from the newspaper *Handelsblatt* in July 2022 revealed that it was trivial to register a fake pharmacy and issue digital certificates, even when a residential apartment address was used. The cryptographic setup used in Germany meant that once issued, these certificates could not be revoked without invalidating the millions issued in that manner.[18] Nor could other European countries, who were part of the shared EU validation system for such certificates, selectively revoke German certificates that were part of proven forgeries.

Other issues in the chain concern the validity of vaccines and the identity of recipients. We know from yellow fever vaccination that falsified vaccines also exist on the market as part of chains that lead to documents for verification.[19] The market for falsified COVID-19 vaccines is large but has been difficult to estimate.[20] Furthermore, many countries did not require a robust process of identity assurance in order to receive a vaccination. There was no guarantee that the person inside a valid vaccination chain, being vaccinated with a valid vaccine, was the person whose name is on the certificate. This makes sense due to a need for rapid rollout, including amongst undocumented individuals who may be persecuted and marginalized by state authorities in other contexts. However, it creates a hole in a chain of trust which cannot be mended by a more solid certification verification process downstream.

In sum, many jurisdictions lacked a reliable and secure chain of trust from the actual act of vaccination through to the digital certificate. This created easy opportunities for forgery within these jurisdictions. The requirement to recognize certificates across borders, a necessity given their main use as international travel documents, meant that even a handful of weak jurisdictions undermined any technical security measures placed on the generation and use of vaccination certificates domestically. While not covered here, the same issues apply for records of testing and records of recovery.

20.2.2 Why Bother?

Just because forgery is possible does not mean that everyone *will* forge documents. The law can always impose serious penalties were fraud to be discovered and that will be enough to dissuade some. There have been penalties and prosecutions for withholding health information at airports since at least 1924, but significant compliance issues have persisted in spite of this.[21] Furthermore, vaccination, testing and recovery are typically all imperfect methods to prevent transmission, and insofar as borders are open to those meeting certain characteristics, pathogens may still enter the country in question. Documentation fraud adds to these errors, but the sum of the intervention of requiring certification may be beneficial if reduction, rather than total security, is an acceptable aim.

An approach of reduction rather than security casts the entire enterprise of verification in a different light. Such an approach would likely be unacceptable for many aims where we try to verify to secure. A nuclear power plant's security systems should not 'reduce' unauthorized entry but prevent the possibility. Yet other environments, such as supermarket self-checkouts or contactless cards, come with an expectation of abuse built into the policy, typically outweighed against a benefit, such as reduced staff cost or greater card usage, and, therefore, more transactions subject to intermediation fees.[22]

Considering vaccine verification in this light raises the question of whether the behavioral consequences of a digital proof infrastructure in a world where dodging it is relatively trivial is enough to justify it being built in the first place. Infrastructures to prove things to people come with serious social consequences. Is this just to give a veneer of fraud protection compared to analogue methods? That a system that many will not understand the workings of might seem more secure than it actually is? Other than the fact that there are many ways to build an opaque computer system, this ignores that systems designed to prove things to people are not just a performance, but they are also performative, in the sense that they have social effects that lead to change.[23]

20.3 Verification's Impacts beyond Biosecurity

A digital verification system is not just icing sugar added to an ICVP to increase its behavioral impact. Digital verification systems do real things in the real world and come with consequences far outside the realm of public health.

20.3.1 Repurposed Infrastructure

The digital systems created to enable verification are often used for purposes beyond that. More broadly, the introduction of technologies at borders typically goes beyond stated purposes to separate out 'legitimate' from 'illegitimate' forms of mobility and to allow surveillance to be practiced both at and away from the border by private actors, such as security firms, as well as state agents.[24] The affordances of digital systems, such as verification, invite extensions and further systems to be built upon them. These are not just systems built upon the vaccination record themselves but systems built on the connection to health databases, the connection to individual identities, the connections to individuals' mobile devices and so on.

One pandemic example is the 'ArriveCAN' app. Originally created as a method to capture data under Canada's Quarantine Act, the app became a mandatory way of submitting such information, first for air travelers in late 2020, then for all travelers in early 2021.[25] However, the Government of Canada stated that the app was 'not only keeping travellers safe, but [was] part of [their] ongoing efforts to modernize the border'. This became apparent, as the mandatory app was extended to contain components of previous border modernization attempts which had failed to get traction, such as the Advance Canada Border Services Agency (CBSA) 'declaration' feature, relating to customs and immigrations, with no link to public health and no debate or discussion.[26] Academic commentators have criticized ArriveCAN's transformation 'from a voluntary app intended to offer an alternative for paperwork to permit contact tracing into a mandatory app that had little connection to public health'.[27]

Another example comes in the form of the German 'Luca' app. This app was launched by a private firm to initially attempt to create a presence-tracing system, where individuals could 'check in' to locations to provide a list of who was there to the venue. This feature was criticized by scholars, who noted its poor design with significant security flaws,[28] and by journalists, who had highlighted the 21 million EUR regional governments had spent on this technology for just a single year of usage, largely in attempt to look active in relation to the federal government in advance of a regional election.[29] A regional court in Rostock later found the purchase of the Luca app by the government there to be illegal.[30] By this time, the app had also expanded beyond its initial features, allowing individuals to integrate their vaccination certificates for the purpose of proof at the border and in shops and restaurants and even to buy tickets to gigs and events through its portal. The firm was effectively attempting to create a public health–related platform to become a technology intermediary across a variety of sectors.

In general, a system that has at its core the ability to prove something to other people forms a strong platform to build on. Once built, such technologies rarely stay still. When a pandemic ends or is at a lull, these technologies enter into confusing situations. They may still have some users and uses. They certainly have maintenance and security issues that need care over time, as operating systems change and new security threats emerge. But maintenance and updating costs money, particularly to maintain infrastructures which may not have a purpose between public health crises. In these situations, maintaining such systems for a crisis with a certain set of functionality can be difficult to justify compared to finding a use for this technology in-between crises. Similarly, when such systems are developed by private actors, they need to locate revenue streams between crises which can keep the organization and the technologies afloat and ready. Preparedness in technologies appears difficult to reconcile with tendencies for 'function creep'.

20.3.2 Exclusionary Standards and Domestic IT Capture

The process around creating the underlying technical set-up for verification of vaccination had significant industry involvement in ways that risked capture of various types.

While an ICVP really only requires common document templates, and relies on stamps and signatures from vaccinating authorities (which may or may not be standardized), a digital verification process typically needs a *public key infrastructure*, or PKI. PKIs provide means to record, distribute and revoke bindings between users and cryptographic keys that relate to them. Public and private keys are core building blocks of cryptography. Entities like a public health authority generate one or more pairs of public and private keys. If they wish to *sign* an event (such as 'Jane Doe received vaccine X on 21.02.21'), they can do so using their private key, which they keep secret and secure. Individuals who want to verify that this was indeed signed by this authority can then check if the signature is valid by comparing it to the alleged signing authority's public key, which by definition should be 'public' and attributable to the authority in question. This makes it important that verifiers have somewhere where they know all the public keys will reliably be placed, alongside notices of revocation, for example, if a private key is hacked so people know not to trust corresponding signatures anymore.

PKIs are a crucial aspect of applied cryptography and one of the hardest to establish and maintain in practice. They are constant targets for surveillance authorities around the world, and the PKIs underpinning encryption on the web are sites of geopolitical tension in Internet governance.[31]

The WHO Smart Vaccination Certificate Working Group indicate in their report that in order to participate in their proposed standard, public health authorities will need to 'have access to a national public key infrastructure', and although they do 'not describe the PKI in detail', they require it to have a wide variety of features.[32] The European COVID certificate, which significantly influenced global standards, could build upon EU countries long having been urged, particularly through successive laws on electronic signatures, to have experience and state capacity in national PKIs.[33] However, countries in the Global South rarely have public sector PKIs established, although they are often part of future digital plans.[34]

The result of this state of affairs is a demand on all countries wishing to participate in international travel to rapidly develop and adopt a complex infrastructure in one of their most sensitive sectors—health. Health informatics is a sector with a lot of promise but also an extraordinary possibility for capture. Building a complex infrastructure during a crisis will only be achievable for poor countries by effectively handing over significant control to private entities. Regardless of the merits or drawbacks of privatization in the health and care sectors, this privatization can really only occur in a rush. The WHO Smart Vaccination Certificate Working Group appeared set up as a sales pitch, with many consultants as members, and the only eligible individuals to apply to this group were those who could at short notice provide a slide deck 'outlining a proposed global interoperability standard for issuing, certifying, and verifying a vaccination event'—a finished, or at least significantly developed, *product*.[35]

In sum, the rushed desire to create *digitally verifiable* vaccination certificates may contribute to rushed procurement of informatics capacity in many countries' public sectors in a way which would seem likely to lead to a loss of control over the problems, capacities, framings and even data flows within those organizations. Such procurement, however, provides little benefits, for the reasons outlined earlier. The extent of this impact requires further country-specific research and follow-up.

20.4 Privacy (Or Rather, Confidentiality) Theatre

As 2020 progressed, questions moved from whether vaccination was possible to how vaccination would affect society. When discussions moved to consider logistical challenges of demonstrating vaccination status, the predominant frame for discussing these questions was one of privacy.

From the perspective of this author, privacy had been a very important frame for pandemic technologies up until this point. We had been involved in the furore around Bluetooth contact tracing technologies, as states had proposed solutions with unnecessary publicity risk, whereas more decentralized solutions that have the same or similar functionality with greatly reduced risks were possible.[36] In the end, decentralized technologies were widely rolled out under the banner of 'Exposure Notification'. These technologies prevented detailed network data of who saw who in society from being accumulated by state actors around the world, including those with lacklustre human rights regimes or those with limited ability to keep this data secure.

Vaccination certificates were not exactly like this. For contact tracing technologies, the functionality itself—notifying individuals subject to a 'risky' encounter—was not particularly controversial. With design precautions, it could be repurposed only in limited ways.[37] For vaccination certificates, the controversial data is not a database of vaccination recipients (which typically exists) nor typically specific vaccination information that a checker may see in the process of checking. The controversial data is the 'tick' or the 'cross': Do you meet the policy of the verifier?[38] Privacy technologies exist which allow individuals to reveal nothing to a verifier except the fact they meet a certain policy that has been set.[39] The issue here becomes less about the data that is used during the process of verification—which is nice to minimize but not the focus—but the functionality that the system enables.

Drawing attention to the verifier's policy should also draw our attention to attributions we may not wish to be possible to be required to attest to. Lifestyle, travel history, occupation, age, socioeconomic grouping—all these have potential causative or correlative links to transmission and vulnerability to emerging pathogens. Individuals have information about most of these characteristics on their mobile devices, whether they inputted it manually or not. If they are not revealed to a querier, should they be able to form part of a policy? We could imagine law and rules governing this, but more than anything, this is governed by the technical possibilities of attesting to these characteristics. A path where individuals can technically attest, even privately and confidentially, to a variety of attributes, may leave us in quite a dark place indeed.

It should, however, be noted that functionality *can* be part of discussions about privacy, particularly when it is conceived of in terms that are relational, about autonomy and self-definition.[40] But in the health domain, privacy is often thought of as *confidentiality*, following the importance of medical confidentiality. Privacy is a concept that captures a bundle of interests. Verification and attestation do the same. Choosing a framing for analysis of the role of verification technologies and infrastructures in society will be key to establishing a wider debate on these practices.

20.5 Concluding Remarks

Perhaps some of these arguments seem moot now. Few countries at the time of writing retain entry requirements around COVID-19. The practical impacts of verification theatre were likely dampened by the United States lacking any national vaccination registry and geopolitically forcing countries to accept trivially forgeable paper cards, regardless of the standards they had invested in or the technologies they had built.

Nevertheless, the saga of verification and its limits in this pandemic should draw our attention more towards the interaction of law and technologies in crises. Both interventions and infrastructures matter, and they cannot be seen apart from each other. We cannot set aside infrastructural considerations simply because urgency calls or ignore the long-term legacies of the systems and schemes that societies dream up simply because we are in a rush. Preparedness should allow us to have deep consideration, and simultaneous discussions, of all issues that matter and which surround a proposed intervention such as vaccine certification. In an age of conspiracy, it can be difficult to speculate about the longer-term development and governance of technological systems without appearing to resort to a 'slippery slope' argument. But the design of infrastructures requires considering use and misuse in the future—how they reconfigure power and facilitate certain policy choices and possibilities over others. The COVID-19 pandemic should sharpen our understanding and sensitivity to the importance of these areas. We need this for both operational preparedness when another crisis arises and to support longer transdisciplinary debates about how to use technologies in societies in crises.

Notes

[1] Max Hardiman & Annelies Wilder-Smith, "The Revised International Health Regulations and Their Relevance to Travel Medicine" (2007) 14:3 *Journal of Travel Medicine* 141.

[2] International Health Regulations 2005, art 36; annex 6–7.

[3] World Health Organization, "Digital Documentation of COVID-19 Certificates: Vaccination Status: Technical Specifications and Implementation Guidance" (27 August 2021) at 1, online: *WHO*. www.who.int/publications-detail-redirect/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1.

[4] e-Health Network, "Guidelines on Verifiable Vaccination Certificates—Basic Interoperability Elements" (12 March 2021), online: *European Commission*. https://health.ec.europa.eu/publications/guidelines-verifiable-vaccination-certificates-basic-interoperability-elements_en.

[5] Razan Osman Abdalla et al, "The Global Health Challenge of Counterfeit Vaccination Certificates: The Case of Yellow Fever Vaccination among Travelers Departing from Khartoum International Airport in Sudan" (2022) 1:4 *Public Health Challenges* e45.

[6] Pierre Saliou et al, "The Scourge of Vaccine Falsification" (2022) 40:14 *Vaccine* 2126.

[7] e-Health Network, *supra* note 4.

[8] As a convenient shorthand, this paper will talk primarily in terms of vaccination and vaccination documentation, which should be seen as inclusive of certificates intending to prove testing or recovery.

[9] Ofcom, "Online Nation 2021 Report" (9 June 2021) at 18, online: *Ofcom*. https://perma.cc/8367-N6WW.

[10] Compare to an analogue phone—which really just consists of a microphone and some buttons that make sounds, with all the processing happening in the telephone network.

[11] Some *Länder* restricted the direct use of *cartes jaunes* from the beginning of 2022; see Charlotte Kurz, "In diesen Bundesländern reicht der gelbe Impfpass nicht mehr" (2 December 2021), online: *Pharmazeutische Zeitung*. www.pharmazeutische-zeitung.de/in-diesen-bundeslaendern-reicht-der-gelbe-impfpass-nicht-mehr-130002/.

[12] Kathy Frankovic, "Are Americans OK with Lying to Get or Avoid Getting a COVID-19 Shot?" (22 October 2021), online: *YouGov*. https://today.yougov.com/topics/politics/articles-reports/2021/10/22/are-americans-ok-lying-get-avoid-covid-vaccine.

[13] Buten un Binnen, "Mehr als 100 Fälle gefälschter Impfpässe bei Bremer Staatsanwaltschaft" (4 January 2022), online: *Radio Bremen*. www.butenunbinnen.de/nachrichten/gefaelschte-impfpaesse-impfung-bremen-polizei-100.html; "Bundesweite Ermittlungen: 12.000 Verfahren zu falschen Impfpässen" (19 January 2022), online: *Tagesschau*. www.tagesschau.de/inland/corona-impfpass-faelschung-verfahren-101.html.

[14] Buten un Binnen, "Ex-Werder-Trainer Markus Anfang legt Geständnis ab" (5 January 2022), online: *Radio Bremen*. www.butenunbinnen.de/sport/werder-bremen-markus-anfang-impfausweis-faelschung-gestaendnis-100.html.

[15] Abdalla et al, *supra* note 5.

[16] This was done transparently, in good faith, and in line with the legal discretion pharmacists had at the time to recognize foreign vaccination certificates, in anticipation that the UK's departure from the EU would cause further recognition challenges for vaccinations.

[17] "Local Pharmacies offer Transcription of CDC Vaccine Cards into EU Digital Standard" (30 March 2022), online: *Stuttgart Citizen*. www.stuttgartcitizen.com/news/local-pharmacies-offer-transcription-of-cdc-vaccine-cards-into-eu-digital-standard/.

[18] Julian Olk, "IT-Experten finden Sicherheitslücke bei Digitalen Impfnachweisen—Ausstellung durch Apotheken gestoppt", online: www.handelsblatt.com/politik/deutschland/corona-pandemie-it-experten-finden-sicherheitsluecke-bei-digitalen-impfnachweisen-ausstellung-durch-apotheken-gestoppt/27443716.html.

[19] Saliou et al, *supra* note 6.

[20] Joseph Amankwah-Amoah, "COVID-19 and Counterfeit Vaccines: Global Implications, New Challenges and Opportunities" (2022) 11:2 *Health Policy and Technology* (The COVID-19 Pandemic: Vaccination Strategies and Global Health Policies) 100630.

[21] Lucy Budd, Morag Bell & Tim Brown, "Of plagues, Planes and Politics: Controlling the Global Spread of Infectious Diseases by Air" (2009) 28:7 *Political Geography* 426.

[22] Emmeline Taylor, "Supermarket Self-checkouts and Retail Theft: The Curious Case of the SWIPERS" (2016) 16:5 *Criminology & Criminal Justice* 552.

[23] Stefania Milan et al, "Promises Made to Be Broken: Performance and Performativity in Digital Vaccine and Immunity Certification" (2021) 12:2 *The European Journal of Risk Regulation* 382.

[24] Louise Amoore, "Biometric Borders: Governing MOBILITIES in the War on Terror" (2006) 25:3 *Political Geography* 336.

[25] Public Health Agency of Canada, "Government of Canada announces new mandatory requirements for travellers to Canada", (2 November 2020), online: *Government of Canada*. www.canada.ca/en/public-health/news/2020/11/government-of-canada-announces-new-mandatory-requirements-for-travellers-to-canada.html; Public Health Agency of Canada, "Government of Canada expands restrictions to international travel by land and air" (12 February 2021), online: *Government of Canada*. www.canada.ca/en/public-health/news/2021/02/government-of-canada-expands-restrictions-to-international-travel-by-land-and-air.html.

[26] Bianca Wylie & Matt Malone, "Canada's ArriveCAN App Is Fostering Inequity at the Border" (9 September 2022), online: *Centre for International Governance Innovation*. www.cigionline.org/articles/canadas-arrivecan-app-is-fostering-inequity-at-the-border/.

[27] Matt Malone, "Lessons from ArriveCAN: Access to Information and Justice during a Glitch" (2023) 35:2 *Intellectual Property Journal* 99 at 115.

[28] Theresa Stadler et al, "Preliminary Analysis of Potential Harms in the Luca Tracing System" (22 March 2021), online: *arXiv*. https://arxiv.org/abs/2103.11958.

[29] Chris Köver & Markus Reuter, "Luca-App: Bund übernimmt Millionenkosten der Länder nicht" (12 January 2022), online: *netzpolitik.org*. https://netzpolitik.org/2022/luca-app-bund-uebernimmt-millionenkosten-der-laender-nicht/.

[30] *Oberlandesgericht (OLG) Rostock* (Urt. v. 11.11.2021, Az. 17 Verg 4/21).

[31] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Newark: John Wiley & Sons, Incorporated, 2020) at 730; Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014) at 95.

[32] World Health Organization, *supra* note 3 at 4.

[33] Stephen Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security" (2005) 11:2 *The Richmond Journal of Law & Technology* 6 at 9.

[34] See, e.g., United Nations Conference on Trade and Development, "Member States of the Economic Community of West African States eTrade Readiness Assessment" (2022) at 41–42, online (pdf): *UNCTAD/DTL/ECDE/2022/1*. https://unctad.org/system/files/official-document/dtlecdc2022d1_en.pdf.

[35] World Health Organization, "World Health Organization Open Call for Nomination of Experts to Contribute to the Smart Vaccination Certificate Technical Specifications and Standards" (2 December 2020), online: *WHO*. www.who.int/news-room/articles-detail/world-health-organization-open-call-for-nomination-of-experts-to-contribute-to-the-smart-vaccination-certificate-technical-specifications-and-standards-application-deadline-14-december-2020.

[36] Carmela Troncoso et al, "Decentralized privacy-preserving proximity tracing" (2020) 43:2 IEEE Data Eng Bull 36; Carmela Troncoso et al, "Deploying Decentralized, Privacy-preserving Proximity Tracing" (2022) 65:9 *Communications of the ACM* 48.

[37] cf Jaap-Henk Hoepman, "Stop the Apple and Google Contact Tracing Platform. (Or be Ready to Ditch Your Smartphone.)" (11 April 2020), online: https://blog.xot.nl/2020/04/11/stop-the-apple-and-google-contact-tracing-platform-or-be-ready-to-ditch-your-smartphone/index.html (presenting examples of repurposing).

[38] Seda Gürses & Michael Veale, "Societal Unknowns of Digital Rule Enforcement?" (10 June 2021), online (video): *YouTube*. www.youtube.com/watch?v=BG3QG7Yza00.

39 For example, attribute-based credentials. See Merel Koning et al, “The ABC of ABC: An Analysis of Attribute-based Credentials in the Light of Data Protection, Privacy and Identity” in *Internet, Law & Politics: A Decade of Transformations*, edited by J Balcells (Barcelona: Huygens Editorial, 2014) 357.

40 Julie E. Cohen, “What Privacy is For” (2012) 126 Harv L Rev 1904; Salome Viljoen, “A Relational Theory of Data Governance” (2021) 131 *The Yale Law Journal* 573; Mireille Hildebrandt, “Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning” (2019) 20:1 *Theoretical Inquiries in Law* 83.