Immunity Passports and Contact Tracing Surveillance

Ignacio Cofone*

24 STAN. TECH. L. REV. 176 (2021)

ABSTRACT

Data-driven contact tracing and immunity certification is being used for the first time in history. This Article assesses these apps' risk and tradeoffs from a private and regulatory law perspective with special attention to privacy and inequality. The Article begins by developing a surveillance-based taxonomy of contact tracing apps and immunity passports. Next, it demonstrates how these apps magnify the problems and limits of consent and anonymization, two important privacy guarantees. It then explores how the interplay of trust and error can pose threats to efficacy, how they raise issues of liability, and how to address them. It then discusses the prospect that these apps cause discrimination and magnify existing inequalities. Underpinning the aforementioned considerations is a balancing assessment that aims to guide policymakers, judges, employers, and individuals in making difficult containment decisions.

TABLE OF CONTENTS

* Assistant Professor and Norton Rose Fulbright Faculty Scholar, McGill University Faculty of Law. ignacio.cofone@mcgill.ca. I'm thankful to Anne Andermann, Stefanie Carsley, Sebastian Guidi, Richard Janda, Bonnie Kaplan, Lara Khoury, Alana Klein, Mason Marks, Sofia Ranchordás, Michael Veale, and the participants of the McGill Research Group on Health and Law event "Privacy, Public Health and the Pandemic" for their helpful comments. I also thank the Stanford Technology Law Review editors for their careful work and Malaya Powers, Ana Qarri, and Jeremy Wiener for their fantastic research assistance. I gratefully acknowledge research support from the Social Sciences and Humanities Research Council.

I. INTRODUCTION

This is the first time that the world meets a pandemic equipped with the ability to use surveillance technology to leverage tracing and identification efforts for containing its spread. In the last year, governments and private actors developed contact tracing apps and digital immunity passports—sometimes called vaccine passports or immunity passes. The decisions made about them now may have consequences for generations.

Digital immunity passports can exempt people from COVID-19-related restrictions, allowing them to travel and, in some cases, engage in otherwise

prohibited activities such as returning to work or school.[1] Proposed as apps that can certify people's immunity status, they facilitate containment as sectors of the population receive vaccines for COVID-19—and will continue to do so as long as fractions of the population refuse the vaccine. Contact tracing apps, in turn, serve a key role in preventing the spread of the virus, significantly enhancing the ability to trace contacts compared to manual tracing.[2] Many regard these enhanced, data-driven methods as key for containing COVID-19.[3] Due to their shared characteristic of using surveillance to contain the pandemic, I call immunity passports and contact tracing apps "containment apps."

Even with developed vaccines, COVID-19 containment efforts are far from over. All states have declared COVID-19 a public health emergency and,[4] in his first week in office, President Biden signed 14 executive actions with containment measures.[5] Immunity passports are not the only measure that remains crucial beyond the rollout of COVID-19 vaccines. Contact tracing will remain a key measure until herd protection is reached, which the World Health Organization (WHO) estimated will not happen for at least another year.[6] Moreover, the lessons learned from the COVID-19 pandemic will be useful for future global health

---

[1] *See infra* notes 62-72.

[2] Jonatan Almagor & Stefano Picascia, *Exploring the Effectiveness of a COVID-19 Contact Tracing App Using an Agent-Based Model*, 10 SCI. REP., Dec. 2020, at 1, 1 ("[M]anual contact tracing can be a time-consuming and inefficient exercise, since models show that the probability of epidemic control decreases rapidly when not enough cases are ascertained via contact-tracing before the onset of symptoms. Technology-based solutions have been proposed to automatise the tracking process, in the form of contact tracing smartphone apps."); Hanson John Leon Singh et al., *Mobile Health Apps That Help with COVID-19 Management: Scoping Review*, 3 JMIR NURSING, May 2020, at 1, 2 (2020) ("Amid the rapidly evolving COVID-19 environment, mHealth [mobile health] apps have been playing an important role in mitigating the COVID-19 response . . . .").

[3] Almagor & Picascia, *supra* note 2, at 1; Singh et al. *supra* note 2, at 2; Yasheng Huang et al., *How Digital Contact Tracing Slowed Covid-19 in East Asia*, HARV. BUS. REV. (Apr. 15, 2020) (providing context on the history and effectiveness of contact tracing apps), https://perma.cc/AZ7X-E98R; Robert A. Fahey & Airo Hino, *COVID-19, Digital Privacy, and the Social Limits on Data-Focused Public Health Responses*, 55 INT'L J. INFO. MGMT., Dec. 2020, at 1, 2 (2020) (adding that there is a deep divide between different philosophies over digital contact tracing); *Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us Out of Lockdown*, UNIV. OXFORD (Apr. 16, 2020), https://perma.cc/N3CL-VNCT.

[4] Emily Berman, *The Roles of the State and Federal Government in a Pandemic*, 11 J. NAT'L SEC. L. & POL'Y 61, 63 (2020).

[5] Christopher Hickey et al., *Here Are the Executive Actions Biden Has Signed so Far*, CNN POL. (last updated Mar. 8, 2021), https://perma.cc/RJQ3-SFYT.

[6] Ludwig Burger & Kate Kelland, *Analysis: Can First COVID-19 Vaccines Bring Herd Immunity? Experts Have Doubts*, REUTERS (Nov. 18, 2020, 1:25 AM), https://perma.cc/PZW2-T3JA (citing the World Health Organization's experts who point to a 65-70% rate as sufficient for herd immunity); *COVID Herd Immunity Will Not Happen in 2021, Says WHO*, DW (Jan. 11, 2021), https://perma.cc/3JCL-SM7S (quoting the World Health Organization's chief scientist).

crises,[7] as this is unlikely to be the last pandemic. This moment is an opportunity to develop robust legal and policy frameworks for containment that will be instrumental when new zoonotic diseases emerge due to climate change—produced by deforestation and new viruses emerging as the polar ice caps melt.[8]

Despite their usefulness in reducing the spread of the pandemic, activists and organizations have warned about the dangers of containment apps, particularly regarding the risks to human rights that can result from their ensuing surveillance.[9] The apps enable governments and private companies across the world to track and surveil citizens and often involve aggregating and combining highly sensitive information such as health information and location. Containment apps present the standard risks that any kind of surveillance poses to human rights.[10] They also present additional risks due to the uneven distribution of their surveillance, which this Article analyzes in terms of types of inaccuracy,[11] trust,[12] and magnifying inequalities.[13]

Many containment apps attempt to address these risks, but they do so with varying success. Moreover, it is impossible for them to eliminate all surveillance risks while remaining functional and useful.[14] The impossibility of removing all risk does not mean that governments should not adopt containment apps. It does mean, however, that containment apps have drawbacks and limitations that prevent them from being a holy grail for containing the pandemic's spread. It also means that it is productive for decision-makers to have a clear picture of what the drawbacks are and how they can be addressed when making implementation decisions. Thus, identifying the existing tradeoffs that these risks pose is needed to enable effective policy responses to the current health crisis. This approach can

---

[7] *See generally* Laura Bradford et al., *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*, 7 J.L. & BIOSCI. 34 (2020) (arguing that COVID-19 digital surveillance is a stress-test for privacy regimes and gaps exist in HIPAA and the CCPA).

[8] James N. Mills et al., *Potential Influence of Climate Change on Vector-Borne and Zoonotic Diseases: A Review and Proposed Research Plan,* 118 ENVTL. HEALTH PERSP. 1507, 1510 (2010); Preneshni R. Naicker, *The Impact of Climate Change and Other Factors on Zoonotic Diseases,* 2 ARCHIVES CLINICAL MICROBIOLOGY, 2011, at 1, 3–4.

[9] *COVID-19, Surveillance and the Threat to Your Rights*, AMNESTY INT'L (Apr. 3, 2020, 11:19 AM), https://perma.cc/CF8R-735X ("If left unchecked and unchallenged, these measures have the potential to fundamentally alter the future of privacy and other human rights."); Jessica Davis, *ACLU, Scientists Urge Privacy Focus for COVID-19 Tracing Technology*, HEALTH IT SEC. (Apr. 20, 2020), https://perma.cc/NZZ3-6MJ8 (focusing on the possibility of "mission creep").

[10] *See* discussion *infra* Part III.

[11] *See* discussion *infra* Part IV.A.

[12] *See* discussion *infra* Part IV.B.

[13] *See* discussion *infra* Part IV.C.

[14] *See* discussion *infra* Part II.A.

assist state governments in developing containment policies that are more likely to be widely accepted as a consequence of minimally encroaching on privacy rights.

A tradeoff-based approach is also useful for individuals. Many do not use containment apps because they do not fully understand their privacy tradeoffs or because they believe that decision-makers have not addressed these tradeoffs appropriately.[15] A fuller understanding of risks can help people in their decision-making and assessment of their skepticism about surveillance. Considering containment apps' consequences and offering a tradeoff-based approach can be useful for navigating a polarized debate.

Because of their shared characteristic of relying on surveillance to contain the pandemic's spread, contact tracing apps and immunity passports have in common key considerations regarding consent, anonymity, accuracy, trust, and inequality, and key elements for legal and policy analysis. The experience with contact tracing apps has lessons about surveillance as a tool to contain a pandemic that apply to immunity passports. When contact tracing apps began to emerge, it was reported that "[s]ome activists worry that the apps could start as a tool to help track the contacts of newly infected patients but end up as de facto 'immunity passports', with citizens required to show their health status on their smartphones before they can use public transport or attend a football match."[16] That moment has now arrived.

This Article develops a taxonomy of containment apps, analyzes their privacy promises, and presents the key surveillance-related risks that they can produce and must address, such as furthering marginalization and inequality. It then explores the proportionality concerns these apps raise. To do so, it builds on the Fair Information Practice Principles, which underlie statutory privacy law, the policy experiences with contact tracing thus far, and past containment experiences such as the HIV epidemic and yellow fever. By doing so, it provides guidance on how to regulate contact tracing apps and immunity passports and

---

[15] *See* Baobao Zhang et al., *Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic*, 15 PLOS ONE, Dec. 23, 2020, at 1, 1 (showing that support for contract tracing apps was relatively low by December 2020, respondents had more concerns for centralized apps than they did for decentralized ones, and respondents had greater support for expanding manual contact tracing than for any app); Kat Jercich, *Survey Says Majority of Americans Won't Use COVID-19 Contact-Tracing Apps*, HEALTHCARE IT NEWS (June 16, 2020, 3:45 PM), https://perma.cc/9YV3-LQ9R.

[16] Patrick McGee et al., *Coronavirus Apps: The Risk of Slipping into a Surveillance State*, FIN. TIMES (Apr. 27, 2020), https://perma.cc/WG7U-DMZK.

provides a roadmap that can be used for analyzing measures to contain future public health crises.

The next Part develops a taxonomy of containment apps and explains how their different versions function, as well as the consequences for surveillance. Part III presents an overview of the human rights concerns that are raised by this type of surveillance and discusses two measures to curb surveillance that containment apps present: consent and anonymity. Because these guarantees are frequent in privacy law, the Article analyzes their potential and limitations in the context of containment apps. Part IV analyzes containment apps' uneven distribution of surveillance: imbalance in types of inaccuracy, poorly calibrated levels of trust in the apps' outcomes, and the magnifying of existing systemic inequalities. Part V brings these considerations together to shed light on how balancing and proportionality exercises for containment apps should proceed. Part VI concludes with policy recommendations for containment apps.

II. A SURVEILLANCE-BASED TAXONOMY

A. Contact Tracing Surveillance Along Two Dimensions

A key advantage of digital tracing methods is that they reduce the need for public health workers to access testing records and reach out to individuals by phone or email. They also avoid relying on individuals' memory in listing to the manual tracer every person that they have been in contact with during the last 14 days—information that individuals may not even know in the first place.

There are many ways to sensibly classify contact tracing apps. Two distinctions are most relevant in relation to surveillance: one regarding the tracing method and another regarding the matching and storage method.[17]

The first distinction is whether the app collects location data or proximity data.[18] That is, whether the app works based on GPS or Bluetooth. GPS reveals

[17] Lars Baumgärtner et al., *Mind the GAP: Security & Privacy Risks of Contact Tracing Apps*, 19 IEEE INT'L CONF. ON TR., SEC. & PRIVACY COMPUTING & COMM. (TRUSTCOM) 458, 461–62 (2020) ("Basically, contact tracing apps differ in (a) the technology used to measure proximity, and (b) the approach of where and how contacts are stored and processed."); Haohuang Wen et al., *A Study of the Privacy of COVID-19 Contact Tracing Apps*, SECURITY & PRIV. COMM. NETWORKS 297, 309 (Noseong Park et al. eds, 2020).

[18] François Tanguay-Renaud et al., *Test, Trace, and Isolate: Covid-19 and the Canadian Constitution* 6 (Osgoode Legal Stud., Rsch. Paper, 2020) ("Location data is considered highly sensitive from a privacy perspective . . . .").

each device's location. Bluetooth, on the other hand, does not reveal location, but only a device's proximity to other devices.[19]

The sensitivity of health information may be evident to most people, but location data is equally sensitive and equally revealing. Location data reveals "highly sensitive data about people's behaviors, patterns, and personal life . . . ."[20] It not only reveals where you are but also what establishments you go to, who you spend time with, when and for how long you do so, and what kind of activities you engage in, among other personal information.[21] As Justice Sotomayor explained in *US v. Jones*, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[22]

Proximity data, on the other hand, is achieved by tapping into Bluetooth's ability to broadcast a unique identifier for each device called a MAC address. Because Bluetooth projects identifiers within a spatial range, it can tell if two devices were in proximity for a specific amount of time.[23] Many contact tracing apps use Bluetooth to exchange "tokens," which are temporary identifiers generated by the device.[24] The device keeps a list of tokens it generated and a list of the tokens with which it recently came into contact.[25]

When a user logs a positive COVID-19 test result into an app that uses proximity data, they share their recent tokens with the app, thereby alerting the app of others who may have been infected.[26] The app then notifies those who were recently in close contact with that person and have also downloaded the

---

[19] *How Does Bluetooth Work?*, SCI. AM. (Nov. 5, 2007), https://perma.cc/MUD5-343L.

[20] Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, FUTURE PRIV. F. (last updated Dec. 17, 2020), https://perma.cc/PZ4T-3YVA.

[21] *See* Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1496 (2018) (demonstrating this with a hypothetical example).

[22] United States v. Jones, 565 U.S. 400, 415 (2012).

[23] *Bluetooth Tracking and COVID-19: A Tech Primer*, PRIVACY INT'L (Mar. 31, 2020), https://perma.cc/W994-MTCA ("Bluetooth tracking is done by measuring the Received Signal Strength Indicator ('RSSI') of a given Bluetooth connection to estimate the distance between devices.").

[24] *Id*. (adding that exchanging tokens is more privacy protective than sharing MAC identifiers).

[25] Andrew Crocker et al., *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, ELEC. FRONTIER FOUND. (Apr. 10, 2020), https://perma.cc/G972-BJRQ.

[26] *See, e.g.*, GOOGLE, EXPOSURE NOTIFICATION: FREQUENTLY ASKED QUESTIONS 2 (2020), https://perma.cc/A7R9-ZMXP (explaining this for the Apple/Google API, on which Bluetooth-based contact tracing apps are built).

app, for example with language along the lines of: "you have been recently in close contact with someone who has tested positive for COVID-19."[27]

Bluetooth-based apps are built on a new Application Programming Interface (API) from Apple and Google.[28] Users of apps based on this API who test positive for COVID-19 can input the positive result in the app with a dedicated one-time code (a "key"). In some of them, those who test positive can also enter the date that they were tested and the time that their symptoms started.[29] The Bluetooth token system avoids using GPS.

While the location data that GPS tracing collects and provides can easily be combined with publicly available data on where businesses are located and with other people's location data, it is difficult to make these inferences based on Bluetooth data.[30] It thus makes it more difficult than GPS to infer personal information.[31] Google and Apple therefore present their system as one that has privacy and security core to design.[32]

The second distinction is between apps that store information needed to identify contacts on each device (decentralized apps) and those that store that information centrally (centralized apps).[33] That is, whether the data collected through Bluetooth or GPS is shared directly among devices, or whether it is transmitted to a central location—such as health authorities—that transmits it to each device.

Some refer to decentralized apps as "exposure notification apps" and reserve the term "contact tracing apps" for centralized apps.[34] Sending all information to

---

[27] Or, alternatively, "you have been recently in close contact with someone who has reported to have tested positive for COVID-19."

[28] Mishaal Rahman, *Here Are the Countries Using Google and Apple's COVID-19 Contact Tracing API*, XDA (Feb. 25, 2021, 2:27 PM), https://perma.cc/5J2H-HUKF.

[29] Canadian Press, *Canada's COVID-19 Alert App Updated to Include More Precise Exposure Information*, CBC NEWS (Oct. 30, 2020, 2:59 PM ET), https://perma.cc/XMB9-85DF (adding that this information can help determine when one was most infectious to others).

[30] EUR. DATA PROT. BD., GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK 7 (2020), https://perma.cc/WD5C-3SWY (explaining that the Bluetooth-only approach is an attempt to avoid the privacy pitfalls of GPS tracing methods).

[31] *See id.* (recommending that proximity and not location data be tracked).

[32] *Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19*, GOOGLE, https://perma.cc/7ZUF-4RH6 ("The Exposure Notifications System was built with your privacy and security central to the design.").

[33] Fahey & Hino, *supra* note 3, at 2 (associating this with "data-first" versus "privacy-first" approaches).

[34] Derek Ruths, *Canada's Proposed Contact-Tracing App Takes the Right Approach on Privacy*, GLOBE & MAIL (June 18, 2020), https://perma.cc/F9UZ-X26H ("[T]here are two very different kinds of

a centralized third party is enormously consequential because it enables the aggregation of information. That entails benefits from an epidemiological perspective and, at the same time, exponentially increases privacy risks, such as the risk of data misuse.[35] Decentralized apps make it more difficult to identify and track individuals based on app data.[36]

The following table sets out the degree of surveillance that results depending on both distinctions, serving as a taxonomy for assessing surveillance risk:

	Decentralized	**Centralized**
Bluetooth	Least surveillance	Medium-high surveillance
GPS	Medium-low surveillance	Most surveillance

TABLE 1: A TAXONOMY OF SURVEILLANCE RISK

The placement of an app in this taxonomy will affect its level of privacy risks. Privacy risks are inevitable because of the nature of the apps' surveillance but they vary according to the extent to which the apps are privacy-conscious. The following two Parts detail how apps address these privacy risks.[37]

B. Applying the Taxonomy

Classifying contact tracing apps under this taxonomy can help identify the extent of surveillance that each app conducts on its users. These vary by state, as states retain police power over public health,[38] even though the federal

apps that are referred to in this overbroad definition: true contact-tracing apps and exposure-notification apps.").

[35] Fahey & Hino, *supra* note 3, at 3 (noting a consequent shift to "privacy-first" approaches).

[36] Ruths, *supra* note 34 ("[L]ittle information is stored or shared with the government or companies, so identifying, tracking or studying people through exposure-notification app data is pretty much impossible."); Tanguay-Renaud et al., *supra* note 18, at 7.

[37] This includes obvious risks such as re-identification (anonymity) and lack of consent, as well as less obvious ones such as inaccuracy risks and discrimination risks that exist because surveillance is often unevenly distributed, disproportionately affecting the most vulnerable. *See* discussion *infra* Parts III, IV.

[38] Edward Richards, *A Historical Review of the State Police Powers and Their Relevance to the COVID-19 Pandemic of 2020*, 11 J. NAT'L SEC. L. & POL'Y 83, 89 (2020).

government has concurrent jurisdiction over other issues related to containing the pandemic.[39]

The apps deployed in Alabama, Arizona, Nevada, New York, and Pennsylvania, for example, fit in the top-left quadrant of this classification—the most privacy-conscious type of contact tracing apps.[40] Abroad, so do Canada's COVID Alert, Austria's Stopp Corona, and Poland's ProteGo, as does the new version of England & Wales' Covid-19 App.[41] These are the least privacy-invasive apps that a government could adopt to trace contacts. That means that they avoid many risks of other alternatives.

Several apps fit in the top right quadrant of the classification, such as Utah's Healthy Together, Australia's CovidSafe, and Mexico's CovidRadar.[42] Bluetooth-based contact tracing apps are more common than GPS-based ones,[43] and many of them store all data centrally. Some apps of this type, such as Australia's app, have been criticized for using such a centralized system.[44] Their supporters have argued that centralized systems are likely to protect people's reasonable expectations of privacy.[45] A centralized system, in turn, provides an added functionality over the first category of apps: aggregating data.

In the bottom left quadrant, using location data in a decentralized system, is Israel's HaMagen.[46] This is the quadrant with the fewest apps and no American app fits in this category.[47] A possible reason for this is that the functional benefits of location data pay off when they are stored centrally and can be aggregated. If

---

[39] Berman, *supra* note 4, at 64–75.

[40] Laura Hecht-Felella & Kaylana Mueller-Hsia, *Rating the Privacy Protections of State Covid-19 Tracking Apps*, BRENNAN CTR. FOR JUST. (Nov. 5, 2020), https://perma.cc/A4N9-GGQE (categorizing apps deployed in the United States by privacy protection).

[41] *See generally* Wen et al., *supra* note 17, at 309 (categorizing dozens of contact tracing apps according to, inter alia, their tracing and storage methods).

[42] Wen et al., *supra* note 17, at 309; Hecht-Felella & Mueller-Hsia, *supra* note 40.

[43] Wen et al., *supra* note 17, at 309.

[44] *See* Kobi Leins et al., *Tracking, Tracing, Trust: Contemplating Mitigating the Impact of COVID-19 with Technological Interventions*, 213 MED. J. AUSTL. 6, 7 (2020) ("[T]he central authority [of Australia] can monitor whether the app is being used in at least 2 hourly increments, and possibly as frequently as every 9 minutes . . . .").

[45] *But see* Marion Oswald & Jamie Grace, *The COVID-19 Contact Tracing App in England and 'Experimental Proportionality*,' 1 PUBLIC L. 27, 32 (2021) (arguing that centralized systems are more likely to engage article 8 of the European Convention on Human Rights than decentralized systems); R (W, X, Y and Z) v. Secretary of State for Health [2015] EWCA (Civ) 1034, [44]–[45] (Eng.) (holding that NHS data on individual debtors who owed fees to hospital departments were not protected because patients were informed that their data would be transferred to the Home Office for immigration control purposes).

[46] Wen et al., *supra* note 17, at 309.

[47] *See id*.

one is designing a more privacy-protective, decentralized app, one might as well use the less invasive Bluetooth data.

On the bottom right quadrant one would place states using Care19 Diary, which are North Dakota, South Dakota and Wyoming, as well as, abroad, Argentina's CUIDAR, Singapore's TraceTogether, and Taiwan's TRACE.[48] Apps that operate in this way rely on high trust in the adequate use of the aggregated information, as they do not keep information from state authorities.[49] Germany initially had this design until it moved to a decentralized approach after receiving heavy criticism.[50] On the upside, these apps facilitate detecting trends.[51] On the downside, they are the most privacy-invasive and present more intensely the problems identified in Parts III and IV.

The apps that have been used so far across states can be classified in this taxonomy:

	Decentralized	**Centralized**
Bluetooth	AL, AZ, NV, NY, PA (various apps)	UT (Healthy Together)
GPS	[no U.S. apps]	ND, SD, WY (Care19 Diary)

TABLE 2: AN APPLICATION OF THE TAXONOMY

These apps have important differences in how they relate to privacy. However, to functionally perform the task of tracing contacts, they also have much in common. Because of their functionality, surveillance risks inevitably remain. Some surveillance risks can be avoided with tradeoffs, and others are

[48] C. Jason Wang et al., *Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing*, 323 JAMA 1341, 1341–42 (2020) (categorizing Taiwan's TRACE while referencing big data analytics); Wen et al., *supra* note 17, at 309 (categorizing Singapore's Trace Together); Felella & Mueller-Hsia, *supra* note 40 (listing the states which use Care19Diary).

[49] Hyunghoon Cho et al., *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*, ARXIV 1, 3 (March 30, 2020) (adding that communities differ in the privacy tradeoffs they may be willing to make).

[50] Jessica Morley et al., *Ethical Guidelines for COVID-19 Tracking Apps*, 582 NATURE 29, 31 (2020).

[51] *See* Andreas Kluth, *If We Must Build a Surveillance State, Let's Do It Properly*, BLOOMBERG (Apr. 22, 2020, 10:30 PM PDT), https://perma.cc/P9BJ-CE83 (adding that Taiwan also assembled various government databases, such as travel and health records, and added them to the aggregated data that the app produced).

inherent to functioning contact tracing apps. The following Parts explore these risks.

C. How Immunity Passports Fit

1. A New Type of Digital Containment

Immunity passports are apps that offer data-based assessments of COVID-19 immunity status. They aim to identify those with immunity to allow countries to progressively scale back shutdown measures and open the economy safely,[52] possibly allowing those certified as immune to engage in more activities than the general population. Such data-based assessments usually mean that the immunity passport can collect and aggregate information regarding immunity from health databases. An immunity passport could gather, for example, information on who was vaccinated, who was shown to have antibodies in a blood test, who had a recent negative polymerase chain reaction (PCR) test, or who tested positive for COVID-19 and subsequently recovered.[53]

Early on, a number of governments suggested that they may use immunity passports based on serology tests, which detect antibodies in blood.[54] This idea was delayed during 2020 due to uncertainty regarding whether and for how long people who contracted COVID-19 are immune from contracting it again, the uncertainty of serology tests, and the high monetary cost of performing such tests for large sections of the population, as warned by the WHO.[55] But the rollout of vaccines provides an alternative method for immunity passports that is not based on the detection of antibodies and avoids those problems. Data about who is vaccinated is more certain than data about recovery. And, unlike data from

---

[52] Aaron Schwid & Tom Frieden, *How to Reopen the Economy Safely? Immunity Passports*, WASH. POST (Dec. 21, 2020, 6:53 AM PST), https://perma.cc/2D3L-93QB (referring to immunity passports "as a form of proof of immunity"); Rashid A. Chotani et al., *'Immunity Passport' Key to Containing Spread of Coronavirus*, UPI (Apr. 30, 2020, 8:11 AM), https://perma.cc/V483-L7H3 (referring to immunity passports as the "solution" to Covid-19 related problems).

[53] *E.g.*, *FAQ*, IMMUNITYPASSPORT, https://perma.cc/C8FV-7WCB (last visited Jan. 22, 2021).

[54] *"Immunity passports" in the Context of COVID-19*, WHO (Apr. 24, 2020), https://perma.cc/UNA4-DDUV; Press Release, Stephen M. Hahn, Comm'r of Food & Drugs, Food & Drug Admin., Coronavirus (COVID-19) Update: Serological Tests (Apr. 7, 2020), https://perma.cc/RJ4W-VRMB.

[55] WHO, *supra* note 54. ("There is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection."). *See also* Alexandra L. Phelan, Comment, *COVID-19 Immunity Passports and Vaccination Certificates: Scientific, Equitable, and Legal Challenges*, 395 LANCET 1595, 1597 (2020) ("Given current uncertainties about the accuracy and interpretation of individual serology testing, immunity passports are unlikely to satisfy this health rationale evidentiary burden . . . .").

antibody tests, governments can collect vaccine data at a low cost. Consequently, numerous companies, consortiums, and non-profit actors have developed immunity passports.[56] Like contact tracing apps, immunity passports aim to curb the virus' spread, but instead of doing so by identifying who may have been infected, they attempt to identify who would not be. Immunity passports, in that sense, can be seen as diametrically opposed to contact tracing apps.

Most immunity passports are encrypted end-to-end (a system in which only the communicating users can access the messages) and have the data controlled by the user.[57] That is, only the user inputs data into the system and only the user decides whether to share it. Some immunity passports store the data in the blockchain, [58] a system of recording information that makes it difficult or impossible to change the record. Users can then share information on their immune status through the app. Some apps, for example, use a QR code.[59] Some of these applications change the QR code at regular intervals—similarly to tokens in contact tracing apps—to ensure that the information is updated.[60] Depending on the immunity passport's use, this information is meant to be shown to border authorities (if used for international travel) or to employers, authorities, or even acquaintances (if used for internal restrictions).

2. Their Fit in a Surveillance-based Taxonomy

The first two countries to implement some sort of immunity passports have been Iceland and Hungary. The former has used it to exempt citizens from in-country restrictions, such as mask mandates, and the latter has used it to determine who is allowed in the country for tourism.[61]

---

[56] *See, e.g.*, Brian Horowitz, *Data Privacy Startup Skyflow Jumps into Digital Health Passport Market to Help Public Spaces Reopen*, FIERCE HEALTHCARE (Feb. 3, 2021), https://perma.cc/3DEV-E7WQ (introducing immunity passport app Skyflow); *UK's Open University Unveils COVID-19 Immunity Certification Blockchain App*, LEDGER INSIGHTS (Apr. 29, 2020), https://perma.cc/7AMC-PKAV (describing The Open University's recently unveiled prototype).

[57] FAQ, *supra* note 53. ("All interactions are encrypted and all queries are traceable and verifiable.").

[58] *European Consortium Develops Blockchain COVID-19 Immunity Passport*, LEDGER INSIGHTS (May 22, 2020), https://perma.cc/EF4A-VU9P (adding that the consortium which develops these apps stated that the passport is compliant with Europe's General Data Protection Regulation).

[59] *Id*.

[60] *See, e.g.*, *Introduction to CoronaPass*, CORONAPASS, https://perma.cc/TSG2-6ZMR; Bizagi, *Introduction to CoronaPass – Powered by Bizagi*, YOUTUBE (June 22, 2020), https://perma.cc/896R-HUAZ.

[61] Scott McLean & Florence Davey-Attlee, *'Immunity Passports' Are Already Here. But They Come*

These illustrate the two models for immunity passports that depend on their use: domestic and international. Examples of domestic immunity passports are Denmark's CoronaPass,[62] Brunei's BruHealth,[63] Saudi Arabia's Tawakkalna,[64] and Estonia's Immuunsuspass.[65] Examples of international ones are Malaysia's and Singapore's Immunitee Health Passport,[66] and Greece's application.[67] The European Union has recently proposed the Digital Green Certificate, which would also be used for travel among member states.[68] The International Air Transport Association, similarly, is proposing the use of a "travel pass" based on immunity passports to certify which potential passengers have been vaccinated.[69]

In the U.S., New York has been the only state so far to roll out an immunity passport. The app, called Excelsior Pass, uses a QR code for vaccination

with Warnings, CNN (Dec. 7, 2020), https://perma.cc/C2PR-57FW (noting that Iceland also grants citizens with "immunity passports" permission to ignore the nationwide mask mandate).

[62] Rory Cellan-Jones, *Covid Passports: What Are Different Countries Planning?*, BBC NEWS (Mar. 26, 2021), https://perma.cc/7B5F-7MUC; *Denmark, Sweden to Issue Digital Vaccine 'Passports,'* FRANCE24 (Feb. 5, 2021, 3:33 AM), https://perma.cc/WV8R-NAU6.

[63] *BruHealth*, MINISTRY OF HEALTH BRUNEI DARUSSALAM, https://perma.cc/DL9H-SFBW; Shareen Han, *Gov't Rolls Out BruHealth Contact Tracing App as Restrictions Loosened*, SCOOP (May 14, 2020), https://perma.cc/M34K-XRUE.

[64] Tuqa Khalid, *Coronavirus: How to Use Saudi Arabia's 'Tawakkalna' App to Get Movement Permits*, ALARABIYA NEWS (May 26, 2020), https://perma.cc/4F52-UXJF. *See also International Monitor: Vaccine Passports and COVID Status Apps*, ADA LOVELACE INST. (June 22, 2020), https://perma.cc/F3DE-FDBU.

[65] Tarmo Virki, *Estonia Starts Testing Digital Immunity Passport for Workplaces*, REUTERS (May 22, 2020, 11:12 PM), https://perma.cc/G24E-45FK; *Estonia Tests Virus 'Immunity Passport' App*, MED. XPRESS (June 5, 2020), https://perma.cc/6UX3-MVBU.

[66] Roy Chiang, *Malaysia's First Health Passport, Immunitee Formally Accepted in Singapore*, MOBI HEALTH NEWS (Mar. 1, 2021, 3:42 AM), https://perma.cc/HJU7-A5AG (clarifying that it is for travel to Singapore only).

[67] Kyriakos Mitsotakis, *To Get Europe Moving Again We Must Act Now on Vaccination Certificates*, EURACTIVE (Jan. 21, 2021), https://perma.cc/KR6A-Z384; *Greece Issues COVID Vaccine Certificates to Those Who Have Had Both Doses*, EURONEWS (last updated Feb. 23, 2021), https://perma.cc/Q82G-H5RZ; *Greece and Israel Sign Common Vaccination Passport Deal*, ONLINE VISA (Feb. 9, 2021), https://perma.cc/EC6H-8689.

[68] *COVID-19: Digital Green Certificates*, EUR. COMM'N, https://perma.cc/NZ6S-XKCS. *See also* Press Release, Eur. Parliament, *Parliament Fast-Tracks Procedure to Adopt Digital Green Certificate by June* (Mar. 25, 2021), https://perma.cc/KPC6-65AR.

[69] EUR. COMM'N, *supra* note 68; Eur. Parliament, *supra* note 68. *See also* Justin Meneguzzi, *Will You Need an 'Immunity Passport' to Travel?*, BBC (Aug. 31, 2020), https://perma.cc/JB9W-KD6Q (asking whether immunity passports are the "ticket to reviving the travel industry").

certification, cross-referencing patient data with state health records.[70] The pass is meant to be shown at participating businesses, which can scan the QR code with a mobile phone or tablet,[71] or other third parties.[72] California has expressed interest in implementing an immunity passport but has not done it so far.[73] On the other end of the spectrum, the governors of Arizona, Florida, Montana, Idaho, and Texas have signed executive orders forbidding them.[74] Although it is an open question whether any state or the federal government would impose mandatory immunity passports, doing so is unlikely given that contact tracing apps—and, at times, even face masks—have been optional.

Another way to distinguish between these apps is the type of data that they use. In terms of the taxonomy presented above, the distinction between centralized and decentralized apps is most relevant for immunity passports. Immunity passports can be considered centralized when they store all reference data in one database and the app is a means to access that information. They can be considered decentralized when they authenticate data without storing it centrally by using blockchain—or another distributed ledger with encryption between nodes. For example, if someone with a decentralized immunity passport goes to a vaccination site, the site will generate a code to represent the information that the person has been vaccinated. The code can then be stored in the Blockchain and, when the person boards a plane, the airline can verify that the code is authentic. Among the examples of immunity passports above, the proposed European Union Digital Green Pass is decentralized; New York's Excelsior Pass, on the other hand, is centralized.

The GPS-Bluetooth distinction is less relevant for these apps because all existing immunity passports can reveal location when scanned. However, continuous tracking is not necessary for immunity passports to function as it is

---

[70] Karen Weintraub & Elizabeth Weise, *New York Launches Nation's First 'Vaccine Passports.' Others Are Working on Similar Ideas, but Many Details Must Be Worked Out*, USA TODAY (last updated Apr. 1, 2021, 5:03 PM ET), https://perma.cc/8HSW-JXWS.

[71] *Excelsior Pass*, N.Y. STATE, https://perma.cc/NH5Y-LX9X.

[72] *Excelsior Pass Terms of Use*, N.Y. STATE, https://perma.cc/XN58-RZB2.

[73] A.B. 2004, 2019-2020 Reg. Sess. (Cal. 2020) ("COVID-19 test results or other medical test results may use verifiable credentials, as defined by the World Wide Web Consortium (W3C), for the purpose of providing test results to individuals."); Adam Schwartz, *No to California Bill on Verified Credentials of COVID-19 Test Results* (May 20, 2020), https://perma.cc/Q2TS-CZBW.

[74] Exec. Order No. 2021-09 (Ariz. Apr. 19, 2021); Exec. Order No. 21-81 (Fla. Apr. 2, 2021, 12:25 PM); Exec. Order No. 7-2021 (Mont. Apr. 13, 2021); Exec. Order No. 2021-04 (Idaho Apr. 7, 2021); Exec. Order No. GA-35 (Tex. Apr. 5, 2021, 1:30 PM).

for contact tracing apps. Distinguishing immunity passports based on unnecessary location tracking entails separating those that just reveal location when scanned from those that continuously track users' location through GPS.[75] Saudi Arabia's Tawakkalna app, for example, must be connected to GPS at all times to work, doing continuous tracking.[76] But New York's Excelsior Pass and the European Union's Digital Green Pass do not, and they even have an option to be printed—making it impossible to track location outside the moments where the QR code is scanned.

The most relevant distinction as to the type of data that the passports use is what sources of immunity they certify. From the apps discussed above, those from Bahrain, Brunei, Estonia, Greece, and Saudi Arabia are based on vaccine data only, working as digital vaccination certificates. New York's Excelsior Pass recognizes vaccine data and negative PCR results. Other apps not yet incorporated by any country, such as one developed by a French-Swiss-Estonian consortium, also certify immunity based on antibody test results.[77] The Danish app recognizes all three types of data: vaccinations, who has developed antibodies, and who tested negative recently. The EU Digital Green Pass, similarly, recognizes vaccination data, negative PCR results, and proof of having recovered from COVID-19 recently. As discussed below, the choice about which data to use is highly consequential for equity.[78]

Immunity passports and contact tracing apps have one key aspect in common. They both aim to curb the virus' spread through selective surveillance. Immunity passports are to vaccine certificates what contact tracing apps are to manual contact tracing: a new data-driven way to implement the containment technique. This leads to both kinds of apps having common elements in their risk tradeoffs—and some important differences. The next two Parts explore these.

---

[75] Some prototypes go further and collect other types of data. For example, one developed by the United Kingdom's Open University captures a host of data, including various types of identity data, such as identifying photos in a "personal data store" that is stored locally on each device. *UK's Open University Unveils COVID-19 Immunity Certification Blockchain App*, LEDGER INSIGHTS (Apr. 2020), https://perma.cc/7AMC-PKAV (describing The Open University's recently unveiled prototype).

[76] Khalid, *supra* note 64. *See also International Monitor: Vaccine Passports and COVID Status Apps*, *supra* note 64.

[77] *European Consortium Develops Blockchain COVID-19 Immunity Passport*, *supra* note 58.

[78] *See infra* Part IV.C.

III. GUARANTEES AGAINST SURVEILLANCE ARE VARIABLE

A. Why Privacy Guarantees Are Necessary

To contextualize the measures that containment apps take for curbing surveillance, it is important to understand when and how surveillance poses a problem: the problem of privacy harms.

Revealing information is not necessarily bad. Disclosing information about contagion with others who may have been exposed is exactly what one hopes contact tracing does. The harms to privacy interests that surveillance creates are produced by revealing, together with this information, other information that could be harmful to the person, such as their habits, preferences, or the company they hold.[79] Privacy harm is largely about disclosing, together with the relevant information, other irrelevant information.[80] That is the surveillance that well-designed systems minimize.

This is directly relevant to distinguishing between types of containment apps. Location reveals other information that is irrelevant for containment but can produce privacy harms. People's location data reveals, for example, their habits and preferences. While proximity data does not reveal location, it still produces a trail of people who the individual was in contact with, when, and for how long,[81] which may also reveal sensitive information.

Privacy risk is also relevant to immunity passports, which contain not only sensitive information that is revealed to the apps directly but also sensitive information that is inferred. Immunity passports reveal to others health information and other sensitive information that is indirectly related to health

---

[79] Ignacio N. Cofone, *Nothing to Hide, but Something to Lose*, 70 TORONTO L.J. 65, 72–77 (2020) ("Those who are persuaded by the "I have nothing to hide" argument . . . tend to claim that people have no privacy disutility from affirmatively sharing information with others. This could be true for some people and for some pieces of information . . . But this does not seem to be true across the board, and these are rarely the kinds of situations that are regulated by information privacy law.") [hereinafter Cofone, *Nothing to Hide*]; Ignacio N. Cofone, *A Healthy Amount of Privacy: Quantifying Privacy Concerns in Medicine*, 65 CLEV. ST. L. REV. 1, 6–8 (2017) (discussing the difficulties in quantifying privacy concerns relating to health data in the evaluation of health policies and proposing how to do so through QALYs).

[80] Cofone, *Nothing to Hide*, *supra* note 79, at 81–83 ("Because pieces of information are often bundled together, the disclosure of relevant information can also imply the disclosure of information that is irrelevant to decision-makers, but which the individual in question might prefer to keep private.").

[81] François Tanguay-Renaud et al., *supra* note 18, at 7–8 ("[I]f a match occurs a user gets notified through the app but does not receive information about the infected person apart from the day of the contact, its length, and the Bluetooth signal strength (in order to deduce distance from the contact).").

that might otherwise be kept private and which an individual may not have otherwise consented to sharing. Some privacy issues can be mitigated by design, as discussed below, but others are inevitable. Even besides the information contained in the app, for example, information can be inferred from merely having the app. When given to those who were vaccinated before widespread vaccine availability, immunity passports can reveal individuals' membership to groups with vaccine priority, such as immunocompromised individuals or those living with HIV.[82]

To curb surveillance while maintaining functionality, containment apps generally rely on two guarantees: consent and anonymity. The next two sections explore them.

B. The Challenges of Reducing Surveillance Through Consent

1. Effective Notice

The first way that containment apps address surveillance concerns is through consent. The use of most containment apps is meant to be completely voluntary. The underlying idea is that, if a user believes that the privacy risks outweigh the apps' benefits, they will not download it.

The consent guarantee comes with a caveat and a limit. The caveat is that, in privacy decisions, users' consent to the collection and use of their personal information does not guarantee that their rights will not be violated.[83] The limit is that the extent to which consent expresses actual voluntariness in most of these apps is questionable.

Valid consent requires effective notice: the Federal Trade Commission has held that notices to users that are vague about an element or practice that is likely

---

[82] People who live with HIV and are under effective antiretroviral therapy are not immunocompromised but may belong to priority lists either due to higher risk of becoming immunocompromised if treatment becomes less effective or due to risks of developing serious conditions if infected compared to the baseline population. *What to Know About HIV and COVID-19*, CDC (last updated Feb. 1, 2021), https://perma.cc/L8YZ-NABU. For example, imagine finding out that a student has an immunity passport—either because you saw their list of phone apps when they placed their phone on the table, because you are a border agent when they are traveling, or because you are their boss at their part-time job where having the app is required to access office space. You will know that person has a trait that justifies getting vaccinated before the rest of their age cohort.

[83] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1892 (2013) (adding that relying on consent "fails to account for the social impacts of individual privacy decisions").

to be material to users vitiates their consent.[84] Consequently, developers should avoid vagueness in notices to their users.[85] For consent to be meaningful, and arguably for it to be valid, each individual has to understand what the collection, use, and disclosure of these data mean. Explaining how exactly the collection, use, and disclosure of these data work in a way that users will understand is genuinely difficult—and developers may not be incentivized to do so.

Effective notice in these systems goes hand-in-hand with transparency. Transparency refers to the understanding of how an algorithm arrives at its output (decision) from its input (the data that it is fed). Lack of transparency makes eventual algorithmic biases difficult to detect and reduce.[86] It is difficult to correct a decision-making process that one cannot access or understand.[87]

Useful disclosure of information, more importantly, could take many forms—it's not an either-or matter.[88] Disclosures could include the data used to train an algorithm, the code, the features, the feature weights, the model, or the output variables. The usefulness of each of these types of disclosures will vary among different groups of people. For an average person, the most useful information will be the features, which are the variables that the model considers. For example, knowing the code of an app will not be very informative for most people, but knowing whether it uses Bluetooth or GPS will. Experts may find the code or the model most useful to audit the process. The code, which is the type of

---

[84] Complaint, *In re* Sears Holdings Mgmt. Corp., FTC File No. 082 3099, No. C-4264 (F.T.C. Aug. 31, 2009). *See also R v Borden*, [1994] S.C.R. 145, 161–62 (holding that consent must be "informed", meaning that individuals must have "sufficient available information to make the preference" to decide whether to waive their right).

[85] The FTC has broad authority over privacy as part of its mandate over unfair and deceptive practices. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–90 (2014).

[86] *See* Miriam C. Buiten, *Towards Intelligent Regulation of Artificial Intelligence*, 10 EUR. J. RISK REG. 41, 51–52 (2019) (explaining how bias can arise in opaque algorithms).

[87] Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18–20 (2014) (arguing that regulatory oversight requires transparency).

[88] *See* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1099–1117 (2018) (examining ways to address the problem of inscrutable algorithmic decision-making); Sandra Wachter et al., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J.L. & TECH. 841, 843 (2018) (arguing that one "could gauge the scope and content of explanations according to the specific goal or action they are intended to support"); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 502–05 (2019) (explaining the possible forms of and alternatives to explanations).

disclosure that usually faces the most resistance to being disclosed, is useful for algorithmic auditing.[89]

This issue relates to the fact that most of the containment apps are developed and owned by private companies.[90] Among those so far deployed, most have made the source code publicly available. This certainly makes them more transparent. The most useful type of notice for users, however, is not the code but the features. Features relate more directly to the information that users input, and they are more easily understandable than the code or the formulas that the app uses to process the information. While making the source code public certainly helps, what is crucial is that users understand how the apps work and on what information they based their estimations.

Given containment apps' complexity and the number of unknowns about how the data could be aggregated and used, meaningful explanation rarely happens. Most apps have minimal explanations for their users, other than providing an introduction to random identifiers when they are used and reassuring a generalized concern for users' privacy.

2. *Effective Choice*

Even if information can be conveyed to users in a way for them to understand all the implications of using the app, there is an additional issue. For consent to be valid, it needs to be "freely and voluntarily given," meaning free from coercion.[91] That is, for consent to be valid, one must ensure that the app is rolled out in a way that is not coercive for the people who consent to its use. Coercion could take place, for example if police action is taken based on the app, such as using data on who is infected to select who to quarantine or to enforce a

---

[89] *See, e.g.*, People v. Super. Ct. ("Chubbs"), 2015 WL 139069 (Cal. Ct. App. 2015); State v. Loomis, 371 Wis.2d 235, 259 (Wis. 2016).

[90] *See* Ciro Cattuto & Alessandro Spina, *The Institutionalisation of Digital Public Health: Lessons Learned from the COVID-19 App*, 11 EUR. J. RISK REG. 228, 235 (2020) ("in the case of the contact tracing app, based on the public statement by Apple and Google, it's envisaged that the contact tracing capabilities will be migrated into the operating systems of mobile phones (which remain the proprietary assets of private companies). This might have security and technical advantages for the functionality of the app; however, it also reduces the visibility of the technical implementation details."). *See also* Marjolein Lanzing, *Contact Tracing Apps: An Ethical Roadmap*, ETHICS & INFO. TECH., at 1, 3 (2020) (discussing the "googlization of health crisis management").

[91] Schneckloth v. Bustamonte, 412 U.S. 218, 222, 234 (1973) (holding that for consent to a search to be considered as voluntarily given, the subject's awareness of the possibility of refusing it is not necessary). *See also* discussion *infra* Part III.B.2.

quarantine—or coupling these data with eventual criminal sanctions.[92] This has been, for example, the case in Taiwan, which used positive results on its app coupled with cellphone tracking to mandate and enforce quarantines.[93] Similarly, China's app, called Health Code, assigns one of three colors to users, which are used to determine who to quarantine and for how long (green for unrestricted movement, yellow for 7 days of quarantine, red for 14 days of quarantine).[94] Hong Kong's StayHomeSafe app, Saudi Arabia's Teetamman app, and Bahrain's BeAware app are not used to determine who must quarantine but are used to enforce quarantines.[95]

This conditioning may be a collateral effect of contact tracing apps, but it is the entire purpose of immunity passports. Designed to certify immunity, immunity passports are meant to allow those who are believed to be immune to perform activities and have access to social participation that those who are not immune would lack. These consequences, which could range from being quarantined or under a curfew for not using the app to being prevented from taking flights or accessing office space, suggest that individuals will not have a meaningful choice to use immunity passport apps and accept the surveillance that comes with them.

The Supreme Court has developed an objective standard for reasonableness into its consent analyses in other areas, such as the Fourth Amendment, which can be applied to containment apps as well.[96] Independent of the chosen reasonableness test, this lack of meaningful choice makes it important to keep unchosen surveillance at a minimum.

---

[92] *See, e.g.*, The Health Protection (Coronavirus, Restrictions) (All Tiers and Self-Isolation) (England) (Amendment) Regulations 2021, SI 2021/97, https://perma.cc/2C4W-3JMM (giving British police authority to track and trace exposure data).

[93] Kluth, *supra* note 51 (applauding the measure and adding that "the whole country voluntarily partnered with the government to create a protean network of databases in which information flows both from the bottom up and from the top down").

[94] *Mobile Location Data and Covid-19: Q&A*, HUM. RTS. WATCH (May 13, 2020, 12:01AM EDT), https://perma.cc/4AY6-MMGM (discussing the measures imposed in Norway, China, and elsewhere).

[95] *Id.*; Dima Samaro & Marca Fatafta, *COVID-19 Contact-Tracing* Apps *in MENA: A Privacy Nightmare*, ACCESS NOW (June 18, 2020, 10:28 AM), https://perma.cc/AZC6-6TN5 (discussing the measures imposed in Bahrain, Saudi Arabia, Qatar, and elsewhere).

[96] Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 Fla. L. Rev. 509, 516-543 (2016) (summarizing the Court's approach to coerced consent). *See also* Schneckloth v. Bustamonte, 412 U.S. 218, 222, 225 (1973) (introducing foundational doctrine on Fourth Amendment consent and coercion); United States v. Drayton, 536 U.S. 194, 205 (2002) (clarifying the role of consent during Fourth Amendment searches by law enforcement).

Even if using the apps is made optional by the government, it is difficult to ensure that users have a meaningful choice and the app is not de facto mandatory. An app can become de facto mandatory if, for example, businesses make installing the app a requirement to enter or receive a service. More problematically, an employer could make the app mandatory for its employees and use it to monitor if employees have been infected.[97] This would follow the trend identified by Ifeoma Ajunwa, Kate Crawford, and Jason Schultz in the employee surveillance context, where consent is steadily turning into a "sanitizing seal of approval."[98]

To ensure that the use of a containment app is truly voluntary, governments should include guarantees that downloading it or using it will not be a condition for social participation or inclusion.[99] Although the examples in the paragraph above are of private actors, some of them, such as airlines and employers, are in a similar position of power as the state with regards to individuals and may warrant a similar test for their ability to coerce individuals into waiving their privacy.

Legislation could address this issue. Other countries that have taken efforts to provide this guarantee. Australia, for example, passed an amendment that outlaws mandating employees or customers to use the country's contact tracing app.[100] No such effort has been made to date in the United States,[101] other than the

---

[97] *See generally* Mahsa Shabani et al., *Reporting, Recording, and Communication of COVID-19 Cases in Workplace: Data Protection as a Moving Target,* J.L. & BIOSCI., Jan.-June 2020, at 1 (discussing employers' duties in reporting and communicating the COVID-19 cases).

[98] Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 774 (2017) (identifying the trend of consent as a seal of approval as being due to power imbalances).

[99] *See* Lanzing, *supra* note 90, at 3 (referring to "societal coercion").

[100] *Privacy Amendment (Public Health Contact Information) Act 2020*, No. 44 (Austl.).

[101] Taylor Eric White et al., *Employer Use of Contact Tracing Apps: The Good, the Bad, and the Regulatory*, NAT'L L. REV. (July 7, 2020), https://perma.cc/64ET-D65V ("there are currently no specific federal- or state-level laws specifically prohibiting employers' use of contact tracing apps."). A reasonable concern could be raised about the constitutionality of such law in terms of the First Amendment. But such legislation would be unlikely to raise First Amendment concerns as it would fall squarely under conduct on the conduct-speech distinction. Even though the distinction can often be unclear, it would be unlikely to present difficulties in this case due to the implausibility of any argument tying the restriction to content. *See* Thomas Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. (forthcoming 2021) (discussing the distinction, which separates what is deemed expressive and is protected by the First Amendment, in terms of First Amendment coverage versus protection, and examining how different types of technology can be classified along such a distinction with particular application to the CFAA). Another concern could be raised based on the Occupational Safety and Health Act, which places a general duty to provide workers an environment free from hazards that can cause death or physical harm—which could be interpreted to include an environment free of COVID-19 through containment apps. *See* 29 U.S.C. § 654. But future and more specific legislation could tailor the scope of, and would not be impeded by, such duty.

state prohibitions of immunity passports. If such a restriction was implemented, it would be difficult to enforce in practice.[102]

Relatedly, if the government or private actors place restrictions on individuals who report positive test results, people may underreport or avoid using the apps all-together. Coercion could come from individuals when people are forced to engage in certain behavior to avoid private discrimination, as described below.[103]

Emphasizing consent, however, can be seen by some as an obstacle to the wide adoption of an app by a country's population, which is an impediment for contact tracing apps' effectiveness. For a contact tracing app to work effectively, it needs buy-in from a substantial percentage of the population. While the initial effectiveness requirement of adoption by at least 60% of the population was disproven as a misunderstanding of the original research,[104] low adoption does make an app less useful.[105] A 60% rate of adoption means that 196.92 million people would have to use it in the United States. A 20% rate of adoption, which would lead an app to detect only 4% of contacts,[106] requires 65.6 million active users. That 20% is far above the most optimistic estimations of adoption to date. These range from 10.6% for Virginia to 1.1% for Wyoming, with other States somewhere in that range, for example New York at 4.5%.[107]

Low adoption leads to the problem of high inaccuracy described below (high false negatives[108]), which may make an app ineffective or even detrimental.[109] If less than 20% of the population uses the app, then someone using the app having contact with a person who is infected and contagious has a lower chance of being alerted of such contact.

---

[102] *See* discussion *infra* Part IV.C.1.

[103] *See* discussion *infra* Part IV.C.2.

[104] Patrick Howell O'Neill, *No, Coronavirus Apps Don't Need 60% Adoption to Be Effective*, MIT TECH. REV. (June 5, 2020), https://perma.cc/2C7V-X4GB (noting that apps have protective effects at lower adoption levels).

[105] *See* Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, SCI., May 8, 2020, at 1, 4 (studying the empirical effects of higher adoption rates on transmission).

[106] Robert Kleinman & Colin Merkel, *Digital Contact Tracing for COVID-19*, 192 CMAJ JUNE 15 2020 E653, E654 (2020) (recognizing this fact as contact-tracing apps' first of five major limitations).

[107] Alejandro de la Garza, *Contact Tracing Apps Were Big Tech's Best Idea for Fighting COVID-19. Why Haven't They Helped?*, TIME (Nov. 10, 2020, 7:00 AM EST), https://perma.cc/M883-HL9D (examining state health authorities' adoption rate statistics).

[108] *See* discussion *infra* Part IV.A (explaining false negatives).

[109] Chiara Farronato et al., *How to Get People to Actually Use Contact-Tracing Apps*, HARV. BUS. REV. (July 15, 2020), https://perma.cc/ZU9A-BWHW.

C. *The Impossibility of Anonymity*

1. *De-identification and Re-identification in Containment Apps*

To minimize unnecessary surveillance, most contact tracing apps come with the promise to anonymize all personal information that they process centrally. This was the explicit promise, for example, of Canada's COVID Alert app during its rollout—which later replaced anonymity promises with more ambiguous language of being privacy-safe after receiving feedback from the Office of the Privacy Commissioner.[110]

De-identifying data is an unequivocal improvement in terms of information security over having it identified. Consequently, sufficiently de-identified data often receives a different legal treatment. For example, the Health Insurance Portability and Accountability Act (HIPAA) authorizes disclosure of de-identified information without the need to re-acquire patient consent.[111]

But it is important to consider that promises of anonymity in these data, when aggregated, are impossible to attain.[112] Truly anonymous data does not exist.[113] One can remove personal identifiers (de-identify) data, but any de-identified dataset can be re-identified with enough effort.[114] A famous Netflix example can illustrate this, where de-identified Netflix movie recommendations were associated with individuals simply by aggregating the (de-identified) movie database with publicly available resources online.[115] These types of re-identification can be done for most types of containment apps.[116] Thus, claiming

---

[110] Josh Ruihley et al., *Continuously Improving COVID Alert*, CAN. DIG. SERV. (July 31, 2020), https://perma.cc/EBU7-CCMC (recognizing that there is some risk that individuals be identified).

[111] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, & 42 U.S.C., C.F.R. § 164.502(d)(1)).

[112] Baumgärtner et al., *supra* note 17, at 461 (explaining how linkage attacks can be used to re-identify individuals).

[113] *See* Gilad Rosner, *De-Identification as Public Policy*, 3 J. DATA PROT. AND PRIVACY, Aug. 2020, at 1, 3–4 (2020) (reviewing scholarship on this point).

[114] Ira S. Rubenstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 704–30 (2016) (adding that harms from failed anonymization may only come to light many years after the fact).

[115] ARVIND NARAYANAN & VITALY SHMATIKOV, ROBUST DE-ANONYMIZATION OF LARGE SPARSE DATASETS 111 (2008 IEEE Symp. on Sec. & Privacy, 2008). *See also* Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), https://perma.cc/K4AD-5SJF (explaining a similar example with America Online).

[116] *See* discussion *supra* Part III.A. *See also* CARMELA TRONCOSO ET AL., DECENTRALIZED PRIVACY-PRESERVING PROXIMITY TRACING (2020) (showing that decentralized, Bluetooth-based contact tracing apps based on the Google/Apple API are not subject to Netflix-type re-identification attacks)

that the data, when aggregated, will be anonymous and therefore not privacy-invasive, is a red herring. The oxymoronic use of the phrase "anonymous identifiers" in centralized datasets is the most glaring piece of evidence of this fact: identification relies on anonymity's imperfection.[117]

The probability of re-identification of any de-identified data depends on the threat model. How likely data are to be re-identified depends on the burdens versus the benefits of re-identification—in other words, how much effort re-identifying that data requires and how valuable the re-identification is.[118] Contact tracing apps' aggregated data are relatively easy to identify because they include granular proximity or location data. They are valuable enough for malicious actors to invest time and money to re-identify, particularly in the case of location data paired with health data. Containment apps that combine health data with location, such as Care19 Diary used in North Dakota, South Dakota, and Wyoming,[119] are thus prime for third-party misuse.[120]

The re-identification risk is significantly bigger for centralized than for decentralized apps.[121] It is bigger for GPS than it is for Bluetooth, but it exists in both—while proximity data is not as easy to re-identify as location data, that does not guarantee anonymity. Users can be identified if proximity data are combined with other data. This is facilitated, for example, when public health agencies solicit zip codes for creating an account for the app.[122] Many contact tracing apps

---

[117] Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Procedural Privacy Protections*, 57 COMM'NS ACM 31, 33 (arguing that anonymous identifiers are "anonymous only insofar as they do not depend on traditional categories of identity while still serving the function of persistent identification.").

[118] L. OU ET AL., BIG DATA 285–308 (2016). *See also* ADAM SHOSTACK, THREAT MODELING: DESIGNING FOR SECURITY (2014); TONY UCEDAVÉLEZ & MARCO M. MORANA, RISK CENTRIC THREAT MODELING: PROCESS FOR ATTACK SIMULATION AND THREAT ANALYSIS (2015).

[119] Hecht-Felella & Mueller-Hsia, *supra* note 40.

[120] *See generally* Rubenstein & Hartzog, *supra* note 114.

[121] Stephanie Rossello & Pierre Dewitte, *Anonymization by Decentralization? The Case of COVID-19 Contact Tracing Apps*, EUR. L. BLOG (May 25, 2020), https://perma.cc/JN24-K9F7 ("As conceded by the DP-3T consortium, under the decentralized solution, the infected user's EphIDs are not completely immune to re-identification attacks. For instance, as clarified in the Data Protection Impact Assessment of the DP-3T protocol, the backend server would be able to re-identify the infected user by storing and processing traffic information about the upload. It follows that, if one takes the above-mentioned zero-risk approach to personal data, the backend server could be deemed to process personal (albeit pseudonymous) data when receiving and sending the infected users' EphIDs.").

[122] JAY STANLEY & JENNIFER STISA GRANICK, THE LIMITS OF LOCATION TRACKING IN AN EPIDEMIC 6 (ACLU, Apr. 8, 2020), https://perma.cc/M5BG-UPJD ("Imagine four different people who all live in ZIP code A and work in ZIP code B: Even if they are not uniquely identified, if one tests positive and their location data is published, the other three may fall under suspicion as well.").

avoid doing this and even go as far as stating that they have no way of knowing their users' location. But even without explicitly requesting location, as the app still requires the internet to be used, containment apps (as many apps in one's phone), could collect one's IP address, knowing which Wi-Fi signal the phone joined, effectively turning it into a location tracking app.[123] The agency running the server receiving the keys will be able to link keys to the IP that is uploading them and know who the individual corresponding to each key is.[124] This makes implementing decentralized, encrypted apps highly consequential for reducing re-identification risks.

2. Inferences and Aggregation

Location data used by immunity passports and GPS-based contact tracing apps are easier to re-identify with a partial lockdown where people visit fewer places than normally. Similarly, information is easier for individuals to infer. If someone who was in contact with three people during the 14-day period receives a notification, (absent false positives[125]) she would have a fair estimation of who the infected person may be. It is easier to identify who triggered a positive notification the fewer people you see.[126] This makes it easier not only during lockdown but also for people who live in areas with a more dispersed population.[127]

Scott Peppet describes these unexpected ways in which the internet of things aggregates data to create new, unexpected inferences as "sensor fusion." As he

---

[123] Andy Greenberg, *Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered*, WIRED (Apr. 17, 2020, 7:00 AM), https://perma.cc/8AH3-2K39 (adding that apps could prevent parties other than those that run the server from eavesdropping on IP addresses). Note that this is not permitted on the Apple and Google Play stores without requesting the user for location. *See Exposure Notification APIs Addendum*, APPLE, at para. 3.3, 3.5 (2020), https://perma.cc/8BTJ-J56J; *Requirements for Coronavirus Disease 2019 (COVID-19) Apps*, GOOGLE SUPPORT, at 3.1, 3.2 (2020), https://perma.cc/SUG9-MRPC. However, it is often difficult for app stores to enforce compliance on third-party developers. Woodrow Hartzog, *Op-Ed: Coronavirus Tracing Apps Are Coming. Here's How They Could Reshape Surveillance as We Know It*, L.A. TIMES (May 12, 2020, 3:00 AM PDT), https://perma.cc/4JNJ-WH7K.

[124] Greenberg, *supra* note 123.

[125] *See* discussion *infra* Part IV.A (explaining false positives).

[126] Yoshua Bengio et al., *Inherent Privacy Limitations of Decentralized Contact Tracing Apps*, 28 J. AM. MED. INFORMATICS ASS'N 193, 194 (2021) (associating this with the "inherent privacy leakages" in contact-tracing apps).

[127] Elizabeth Thompson, *COVID Alert App Could Result in Some People Being ID'd*, CBC NEWS (Aug. 5, 2020, 4:00 AM ET), https://perma.cc/T69B-AGKK (quoting Canada's Privacy Commissioner).

puts it, when connected sensors are used, "everything may reveal everything."[128] Data from sensors such as microphones, cameras, and our phones, combine in unexpected ways. The information that a sensor collects is less important than the information that is inferred with what the sensor collects. That gives users no real choice over their (more important) inferred data.[129] Sensor fusion plays a role in dismantling the anonymity promises of centralized containment apps because it illustrates how easy it is to re-identify people with aggregated information as granular as location (GPS) or proximity (Bluetooth). For example, having four location points is enough to be able to personally identify (that is, name) 95% of people.[130]

Depending on how many people one was in contact with, and how many these others were in contact with, Bluetooth data can also be used to infer location data through what is called a linkage attack.[131] One experiment, for example, placed several Bluetooth devices at different locations of a city to show that a linkage attack on them enables re-identification and profiling.[132] This risk can be lowered by increasing the frequency with which tokens change.[133] In particular, this risk is reportedly lower for decentralized, Bluetooth-based apps built on the Apple/Google API than it is for other apps.[134]

This leads to two counterarguments worth considering regarding anonymity. First, sometimes Bluetooth data's potential to be re-identified by combining it with other data, jeopardizing apps' anonymity guarantees, is quickly dismissed. The dismissal argument usually goes: The app itself uses anonymous identifiers and is therefore still anonymous. It is the app's implementation (combining with other information such as IP or zip code) that makes it not anonymous, not the

---

[128] Scott R. Peppet, *Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 120 (2015) (adding that the "extent to which 'everything reveals everything' is an empirical question").

[129] *Id.* at 91 (examining the extent to which consumers have "real choice" in the context of new automobile purchases and Event Data Recorders).

[130] Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP., Mar. 2013, at 1-2 (2013).

[131] Bennett Cyphers & Gennie Gebhart, *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers*, ELEC. FRONTIER FOUND. (Apr. 28, 2020), https://perma.cc/E52J-JLGN (adding that Apple and Google's system has infected users publicly share their once-per-day diagnosis keys, which is a lower frequency than alternative systems); Bengio et al., *supra* note 126, at 194 (explaining that even the best designed contact tracing apps are vulnerable to linkage attacks and thus pose privacy risks). *See also* discussion *infra* Part III.C.

[132] Baumgärtner et al., *supra* note 17, at 460–62 (highlighting an empirical experiment which demonstrated that linkage attacks can infer location and profile individuals accordingly).

[133] Cyphers & Gebhart, *supra* note 131.

[134] Greenberg, *supra* note 123.

app itself. The implication of this line of thought is that the app is not to blame for the lack of anonymity. This is technically correct, but somewhat deceiving: part of the work of de-identifying any information is placing enough safeguards so that it will not be easily re-identified.[135] And, more importantly, highlighting ease of re-identification is less of a critique of the system itself than it is of the decision-makers who promise anonymity based on the system. The FTC has held that companies are to blame when they make promises to their users that they cannot fulfill, even if the fulfillment of those promises in themselves is not blameworthy.[136]

Second, people sometimes argue that others have been releasing their location (or proximity) data to other apps anyway, and the task of containment apps is more important.[137] This argument is mistaken because previous disclosure does not mean that disclosing the same information again cannot be harmful or is justified. This argument is premised on the common privacy misconception that privacy interests are binary: either information is secret and private, or it is not secret and it is public.[138] But there is no such thing as information so public that it is irrelevant who else acquires it; disclosing information to someone else means expanding the audience for that information and, therefore, increasing the potential for harm.[139]

Finally, and most importantly, anonymizing these data is not only impossible but, even if it were possible, it would not resolve some of the privacy harms that surveillance produces. "Anonymous" data still reveals information and trends about groups.[140] Data that remains de-identified can harm members of those groups by, for example, being used in a discriminatory manner, even

---

[135] Rubenstein & Hartzog, *supra* note 114, at 704–30.

[136] *See In re* Snapchat, Inc., F.T.C. 132 3078 (Dec. 23, 2014) (concluding that Snapchat deceived consumers by attesting that snaps would disappear after a few seconds, even though third-party apps could retain them and users owning old smartphones could take screenshots of them).

[137] Crocker et al., *supra* note 25 (recognizing that this argument is made without making it themselves).

[138] SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 8–16 (2020) (describing and criticizing the paradigm of privacy as secrecy).

[139] Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1049-1053 (2018) ("Informational privacy is not only about having privacy or not. . . .Instead, informational privacy is really about *levels* of privacy."); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) (describing the binary view as one in which "exposure to a limited audience [is treated] as morally equivalent to exposure to the whole world.").

[140] Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 583–90 (2020) (distinguishing between "socially salient" and "non-socially-salient" groups).

unintentionally.[141] Harms in group privacy do not rely on re-identifying individuals: decisions can affect de-identified individuals on the basis of group attributes such as gender, sexual orientation, and political preference.[142] Further, breaches in group privacy can result not only in discrimination, but also in infringements of other constitutional rights such as free speech and freedom of association.[143]

IV. CONTAINMENT SURVEILLANCE IS UNEVENLY DISTRIBUTED

A. Types of Inaccuracy

1. Different Error Rates: False Positives and False Negatives

Algorithms work based on proxies. The effectiveness of any algorithm depends on the strength of the proxies it uses.[144] In the case of Bluetooth-based contact tracing apps, for example, having one's device exchange tokens with a device that registered a positive test result works as a proxy for having been exposed to COVID-19.[145] In turn, a device's Bluetooth signal reaching another one is a proxy for shared air, which is how the virus is centrally transmitted.[146] This allows contact tracing apps, for example, to rule out two people walking past each other as close contact given the low likelihood of transmission.[147] In the case of

---

[141] Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 869–92 (2017) (discussing three different types of unintentional yet discriminatory group privacy harm); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 674 (2016) ("Because the discrimination at issue is unintentional, even honest attempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions. Furthermore, because the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address.").

[142] *See, e.g.*, Kerina Helen Jones et al., *Toward an Ethically Founded Framework for the Use of Mobile Phone Call Detail Records in Health Research*, JMIR MHEALTH UHEALTH, Mar. 22, 2019, at 1, 6 (recognizing that "breaches in group privacy do not rely on the reidentification of individuals"); Baumgärtner et al., *supra* note 17, at 460–62 (demonstrating how a linkage attack can lead to group harm).

[143] *See, e.g.*, Rachel L. Finn et al., *Seven Types of Privacy*, *in* EUROPEAN DATA PROTECTION: COMING OF AGE 3, 7–10 (Serge Gutwirth et al., eds., 2013) (discussing the freedom of speech, of assembly, and more). *See also* Wen et al., *supra* note 17.

[144] Ignacio N. Cofone & Katherine J. Strandburg, *Strategic Games and Algorithmic Secrecy*, 64 MCGILL L.J., 623, 634–636 (2019) (noting that proxies determine the gap between an algorithm's actual and ideal decision).

[145] GOOGLE, *supra* note 26, at 2.

[146] Greenberg, *supra* note 123(citing the TCN Coalition and the Apple/Google joint project).

[147] Tanguay-Renaud et al., *supra* note 18, at 3.

immunity passports, presenting evidence of having received a vaccine or having antibodies detected is a proxy for being immune to the virus.

These are decent, and perhaps some of the most acceptable, proxies available. But, like all proxies, they are imperfect, and it is important to pay attention to the distributional aspects of their imperfections. We should, accordingly, distinguish between two types of errors. False positives are errors indicating that someone was exposed or is immune to COVID-19 when they are not. False negatives are errors indicating that someone was not exposed or is not immune to COVID-19 when they were indeed exposed or are immune. Distinguishing between false positives and negatives is important because they differently impact people's use of containment apps. They have different social costs.

Regarding contact tracing apps, Bluetooth can tell how close you were to someone and for how long.[148] But it does not know if you or they were wearing a mask. It also does not know if there was a plexiglass between you or if you were each inside of your own car, with your windows closed, waiting at a red light next to each other. It does not know when there is a wall, for example between you and your neighbor, and that you do not spend every night sleeping next to them. It does not know that the person who lives below or above you is not in your living room. Although some physical obstacles, such as walls, do slightly decrease the strength of Bluetooth signals, they do not decrease it nearly as much as they stop the virus' aerosol transmission.[149] Using face masks and hand sanitizer, for example, reduces the likelihood of transmission but will not affect Bluetooth signal.[150] These errors are what we call "false positives."

For immunity passports, "false positive" means "mistakenly thinking the person can potentially get infected with the virus when they are immune."[151] Not

---

[148] *Bluetooth Tracking and COVID-19: A Tech Primer*, *supra* note 23.

[149] *Public Health Activity Guidance*, CDC (Apr. 9, 2020), https://perma.cc/CL8U-DH5W (discussing physical barriers as important measures to reduce risk of transmission).

[150] *See Science Brief: Community Use of Cloth Masks to Control the Spread of SARS-CoV-2*, CDC (May 7, 2021), https://perma.cc/B6YH-GD42; Douglas J. Leith & Stephen Farrell, *Measurement-Based Evaluation of Google/Apple Exposure Notification API for Proximity Detection in a Light-Rail Tram* 15 PLOS ONE 1, 12 (Sept. 2020) (performing an experiment on a tram on the Google/Apple API to evaluate when exposure notifications are triggered and identify errors).

[151] Note that defining error rates as "positive" and "negative" is linguistic: any system has type 1 and type 2 errors; which of them we call positive and which we call negative depends on how we define the hypothesis. Here, I defined the hypothesis in such a way for symmetry with contact tracing apps. But, if analyzed in isolation, the errors that I called positive could be called

using the app while immune would create false positives, as would being unknowingly immune—for example when someone has immunity because they developed the disease after becoming infected but they did not know. A less common false negative would be not logging an immunity into the app—unlikely since logging immunity is the point of downloading the app.

2. Error Rates' Differential Behavior

False negatives are less varied than false positives. As far as contact tracing apps are concerned, the more common false negatives would occur when in proximity to an infected individual who does not use the app, has not gotten a test when infected, or has not logged a positive test result into their app. A less common false negative would occur if someone were infected with COVID-19 by touching a surface that an infected person touched recently.[152] If immunity passports are only given to those who are vaccinated, false negatives will occur when the vaccine fails to immunize an individual—that is, the immunity passport erroneously certifies that the person cannot contract the virus. The Pfizer and the Moderna vaccines have a 95% effectiveness rate.[153] This would mean that the immunity passports would have only a 5% false negative rate if implemented 100% correctly—that is, not given to anyone who was not properly vaccinated.[154] If the immunity passports are given more widely, for example based on evidence of antibodies in a blood test, false negatives would occur when the serology test gives a false positive or when the individual was immunized but the immunization wears off over time—for example, it is uncertain how long immunity lasts after recovering from the virus.

---

negative and vice-versa. In such case, the considerations that I explained for false positives would apply to the new "false negatives;" the converse is also true. Those considerations are not essential to the categories of "positive" and "negative" but rather to the types of errors.

[152] We now know that transmission from surfaces is significantly less likely than transmission from people standing close to one another. *Science Brief: SARS-CoV-2 and Surface (Fomite) Transmission for Indoor Community Environments*, CDC (last updated Apr. 5, 2021), https://perma.cc/D7AP-JSSD.

[153] *E.g.*, Peter Doshi, *Pfizer and Moderna's "95% Effective" Vaccines – Let's be Cautious and First See the Full Data*, BMJ OPINION (Nov. 26, 2020), https://perma.cc/C2C8-SDCG (adding that independent scrutiny of the underlying trial data would be beneficial).

[154] This is assuming that no one is naturally immune. The more naturally immune people, the fewer false negatives. If, to give an exaggerated number, 50% of the population were naturally immune because they recovered from the virus recently or for some other reason, then only half of those who were vaccinated but not immunized by the vaccine would present false negatives, so 2.5%.

False positives may have a detrimental effect on people's mental health and businesses' finances.[155] For contact tracing apps: "One or more intentionally false reports of positive tests could have financial and social consequences for businesses or people who either believe they are infected, or whom other people believe are infectious."[156] The same can be said about unintentional false reports. For immunity passports, false positives would delay the lifting of economically costly measures such as shutdowns and curfews for an individual. False positives also matter because they erode trust in the app. If, for example, someone receives many false positives in a contact tracing app while being confident that she is negative, she may not trust what the app says anymore, and the app's usefulness would be undermined if a true positive occurs later.

False negatives, in turn, lead infected people to erroneously think that they are not infected. Consequently, they may not get timely treatment or fail to quarantine and spread the virus to others. False negatives are detrimental to containing the spread of the pandemic. For example, regarding immunity passports, people might expose themselves to situations of transmission more than they otherwise would because they mistakenly think that they are immune. Indeed, an app with many false negatives could be worse than no app at all if people were to ignore symptoms because they trust that they have not been exposed to the virus given the app's results.[157] False negatives, for that reason, are more costly than false positives. Minimizing false negatives rather than false positives is therefore desirable for containment apps.[158]

This cost asymmetry teaches an important lesson for rolling out immunity passports. Deciding who should qualify for immunity passports is a question of balancing false positives and false negatives. Each false negative from an immunity passport (each person mistakenly classified as immune, who could spread the virus) is more socially costly than each false positive (each person who is immune but is not or cannot be certified as such). Therefore, immunity passports should be provided in such a way that they minimize false negatives

---

[155] Lucy Simko et al., *COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences*, ARXIV 1, 5–6 (2020) (arguing that these broader issues such as these must be considered).

[156] *Id*. at 6.

[157] DEPT. HEALTH & SOC. CARE, CORONAVIRUS (COVID-19) SCALING UP OUR TESTING PROGRAMMES, 2020 (U.K.) (discussing test unreliability in terms of false negatives and arguing that an unreliable test is worse than no test at all).

[158] *See id*. *See also* Rebecca Brown et al, *Passport to Freedom? Immunity Passports for COVID-19*, 46 J. MED. ETHICS 652, 652 (2020) (discussing false positives and false negatives in immunity passports).

with less concern for false positives. For example, they should be provided only to those who have received a second dose of the vaccine.

This proposed toggling of error rates' distribution would not be without precedent. Courts and legislatures have considered the distribution of error rates when deciding whether to implement a test on countless occasions. For example, the Supreme Court has held that sniffing dogs' false positive rates at detecting drugs are relevant in determining whether a police officer has probable cause to conduct a search pursuant to the Fourth Amendment.[159] The difference between tests like dog sniffing and algorithms like immunity passports is that, for the former, error distributions are fixed and simply inform adoption while, for the latter, implementation options can alter those error distributions. It is thus desirable to adjust those distributions to the social costs of errors.

This is possible in contact tracing apps as well. In experiments performed on apps based on the Google/Apple API framework, researchers have found different rates of false positives and false negatives on different countries' apps,[160] meaning that it is possible, from a technical point of view, to adjust which types of errors will be more frequent.

B. Trust

1. Calibrating Trust

To a large extent, the cost of false positives and false negatives depends on how containment apps are used by the public. This is because errors become more problematic when an inadequate amount of trust is placed in the app. Cathy O'Neil explains this in terms of the importance of not placing blind faith in data outcomes, which she calls being a data skeptic.[161] The importance of this skepticism increases with high-stakes systems such as containment apps. For

---

[159] *See* Florida v. Harris, 133 U.S. 1050 (2013).

[160] Leith & Farrell, *supra* note 150, at 12 ("We find that the Swiss and German detection rules trigger no exposure notifications on our data, while the Italian detection rule generates a true positive rate of 50% and a false positive rate of 50%. Our analysis indicates that the performance of such detection rules is similar to that of triggering notifications by randomly selecting from the participants in our experiments, regardless of proximity."); Douglas J. Leith & Stephen Farrell, *Measurement-Based Evaluation of Google/Apple Exposure Notification API for Proximity Detection in a Commuter Bus*, ARXIV 1, 1 (2020) (performing the same study on a bus and reaching similar results).

[161] CATHY O'NEIL, ON BEING A DATA SKEPTIC 1 (2013) ("A skeptic is someone who maintains a consistently inquisitive attitude toward facts, opinions, or (especially) beliefs stated as facts.").

these apps to be effective, the right amount of deference must be given to the algorithm.[162] People often defer too much.[163]

If someone does not trust the app's outcome—if there is under-reliance on the app—the whole system becomes unhelpful for them.[164] Algorithmic proxies are of little use if ignored. In containment apps, "[t]he whole system depends on trust. If users do not trust that an app is working in their best interests, they will not use it."[165] This problem becomes dire in a social context where sectors of the country do not trust the federal government, do not believe that COVID-19 is real, believe that it is simply a flu, or believe in conspiracy theories about its origin and spread.

But placing too much reliance on the app is equally problematic.[166] This is because incorporating data-driven systems and relying on their conclusions without considering outside evidence and context is generally counterproductive.[167] Overreliance on an immunity or contact tracing result when there is a false negative might make people less likely to take other health measures because they have received a negative from the system. Overreliance when there is a false positive can impose unnecessary stress on families and overburden the healthcare system. Similar problems in terms of false positives

---

[162] *See* Jack M. Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. 45, 57 (2015) ("Through their interactions with robots and AI systems, people are willing to substitute them for animals or human beings in certain contexts and for certain purposes.").

[163] Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction*, 5 ENGAGING SCI. TECH. AND SOC. 40, 41–42 (2019) (arguing that there are significant negative outcomes to the tendency to over-rely on machines).

[164] Berkeley J. Dietvorst et al., *Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err*, 144 J. EXPERIMENTAL PSYCHOLOGY: GEN. 114, 119–26 (2015) (introducing the concept of algorithmic aversion); Berkeley J. Dietvorst et al., *Overcoming Algorithm Aversion: People Will Use Imperfect Algorithms if They Can (Even Slightly) Modify Them*, 64 MGMT. SCI. 1155, 1156 (2016) (discussing ways to overcome algorithmic aversion); Berkeley Dietvorst & Soaham Bharti, *People Reject Algorithms in Uncertain Decision Domains Because They Have Diminishing Sensitivity to Forecasting Error*, 31 PSYCHOLOGICAL SCI. 1302 (2020) (finding that algorithmic aversion increases in scenarios of uncertainty). *See also* Tanguay-Renaud et al., *supra* note 18, at 9 (an app "might not be effective if citizens do not actually trust it and therefore do not use it").

[165] Cyphers & Gebhart, *supra* note 131 (adding that transparency can promote trust). *See also* Graham Greenleaf & Katharine Kemp, Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing 4 (May 15, 2020) (UNSW Legal Research) (recognizing that the extent that the Australian public's trust in the government's app has an effect on consent and adoption rates).

[166] Rebecca Crootof, *'Cyborg Justice' and the Risk of Technological-Legal Lock-In*, 119 COLUM. L. REV. F. 233, 243 (2019) (noting risks of "overtrust" and "undertrust" and explaining that "To effectively participate in a human–machine team, the person in the loop must have an appropriately calibrated amount of trust.").

[167] *See, e.g.*, Kate Goddard et al., *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. AM. MED. INFORMATICS ASS'N 121, 124–25 (2012) (discussing automation bias).

and false negatives arise if the actors over-relying are not private individuals but public health officials.

A solution to problematic calibrations of trust in a data-driven system is integrating the system into a human-driven process. Such a process, also referred to as having a "human in the loop," is one that enables operators to influence the system.[168] Influence includes the ability to choose whether to follow or override the algorithm's recommended decision and can take many different forms. In short, putting a human in the loop means shifting data-driven systems away from replacing human decision-makers and towards assisting them.[169] As Kiel Brennan-Marquez, Karen Levy, and Daniel Susser put it:

> Sometimes, the human role is largely procedural: for example, pushing a given case up or back in the relevant queue, or deciding which cases merit more institutional resources. Other times, the human role is more dispositive, involving the power to shape outcomes, either in terms of a case's concrete effects (e.g., granting or denying benefits), or in terms of how the outcome is justified, or both. The specifics of the human role may vary, but the key is that a human has some form of meaningful discretion in particular cases.[170]

In the context of contact tracing apps, this means that apps should assist, not replace, human contact tracers and public health officials. Massachusetts, for example, built on this idea when it implemented a program of human contact tracing to leverage the trust relationship that tracers can establish.[171] Human contact tracing not only can mitigate the risks that digital contact tracing poses

---

[168] *See* John Nay & Katherine J. Strandburg, *Generalizability: Machine Learning and Humans-in-the-Loop*, *in* RESEARCH HANDBOOK ON BIG DATA LAW 284 (Roland Vogl, ed., 2021); Rebecca Crootof, *"Cyborg Justice" and the Risk of Technological-Legal Lock-In*, 119 COL. L. REV. 233, 243–49 (2019).

[169] Richard M. Re & Alicia Solow-Niederman, *Developing Artificially Intelligent Justice*, 22 STAN. TECH. L. REV. 242, 282–85 (2019) (discussing ways that labor can be divided between algorithms and humans); ANTHONY NIBLETT ET AL., REGULATION BY MACHINE (30th Conf. Neural Info. Processing Systems, 2016); Benjamin Alarie, *The Path of the Law: Towards Legal Singularity*, 66 U. TORONTO L.J. 443, 446–51 (2016) (explaining this in the context of tax law); Vasant Dhar, *When to Trust Robots with Decisions, and When Not To*, HARV. BUS. REV. (May 17, 2016), https://perma.cc/N9ZK-N5RG (developing possible "automation frontiers" between human and machine-appropriate decision problems).

[170] Kiel Brennan-Marquez et al., *Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision Making*, 34 BERKELEY TECH. L.J. 745, 749 (2019).

[171] Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://perma.cc/KW28-7W8C.

(such as trust, error, and inequality) but can also help in ways that digital contact tracing cannot.[172] "Human contact tracing involves educating people about risks and helping them access social supports as they self-isolate and monitor themselves for symptoms, and ideally are given access to testing even if asymptomatic—this vital component cannot be done via contact-tracing apps."[173]

Integrating the app into a human-driven decision-making process is simpler for immunity passports: these should operate as a guarantee of immunity according to the terms that public health officials have decided, such as receiving the second dose of an approved vaccine. It is less straightforward with contact tracing apps, which should not be used as a reason to have fewer human contact tracers and should be flexible to their informational needs to contain spread. In terms of the taxonomy introduced above,[174] one drawback of Bluetooth-based apps is that they integrate less well with human contact tracers than GPS-based apps do; location logs pose disadvantages from a surveillance viewpoint but they better complement human contact tracers.[175] More broadly, implementing containment apps in a human-driven process is likely to reduce both error rates and the undesirability of how they are distributed.[176]

2. *Consequences for Liability*

These considerations on trust connect to the private characteristic of these apps. Jody Freeman asked almost two decades ago how we can ensure that the intersection between private and public law works when public actors rely on private actors for things that can generate public limitations or individual obligations.[177] This is very much the case of containment apps, and particularly of immunity passports that define the scope of public health restrictions. The way

---

[172] Tanguay-Renaud et al., *supra* note 18, at 4 ("Although contact tracing apps could make some components of contact tracing more efficient, they cannot replace human contact tracing and so need to be integrated into the human contact tracing process.").
[173] *Id*.
[174] *See supra* Part II.
[175] Tanguay-Renaud et al., *supra* note 18, at 7 (explaining how centralized systems provide human contact tracers with more information than they otherwise would have).
[176] *Id*. at 5 (referencing the problem of false positives and negatives, the fact that not everybody has a smartphone, and more).
[177] Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1290 (2003). *See also* Sofia Ranchordás & Catalina Goanta, *The New City Regulators: Platform and Public Values in Smart and Sharing Cities*, 36 COMP. L. SEC. REV. 1, 12 (2020) (discussing the problem of having private companies defining limits in the public sphere and influencing public values).

that these private actors' incentives are aligned with public incentives is chiefly through liability regimes. This connection leads to two questions of liability.

The first question is one of state liability. In light of the considerations above, a reader may ask: Do state public health authorities have a private law duty to warn holders of immunity passports that they are not 100% immune? The short answer is no. As held in *Blessing v. United States*, state authorities will only be held liable if negligence stems from the operational implementation of a policy decision and not the policy decision itself.[178] This is because the policy decision itself requires the state to act in the public interest, which may be antithetical to a judicially-imposed private law duty. [179]

The second is a question of corporate liability, and in particular product liability.[180] Courts have held that drug testing kits manufacturers have a duty to warn law enforcement agencies and officers when and to what extent the test could return false positives and negatives.[181] Although the case law applies only to test kit manufacturers, similar reasons to adopt such a rule apply to developers of containment apps that are endorsed by the government and used for public health. An open question, therefore, is the extent to which containment apps' developers should have an analogous corporate duty to warn the state and federal agencies that endorse them of false positive and negative rates.

If these warnings include data from individuals who had these false positives or false negatives, the disclosures could increase surveillance risks. This issue can be addressed by building on the considerations on transparency as an element of consent discussed earlier and the importance of users' trust. The increase in surveillance risk due to error disclosure could be addressed while achieving the purpose of liability if the duty to warn existed, instead, towards the apps' users.

Apps should be transparent with their users about the types of error and the errors' likelihood for their consensual use to be legitimate. In the absence of this transparency, because of its importance for consent, apps should face liability for

---

[178] Blessing v. United States, 447 F. Supp. 1160, 1170 (E.D. Pa. 1978).

[179] Accordingly, the Federal Tort Claims Act (FTCA) establishes that it shall not apply to "[a]ny claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, whether or not such statute or regulation be valid, or based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused." 28 U.S.C. § 2680.

[180] *See, e.g.*, Maryam Casbarro, *Litigation Risks for Contact Tracing Technology*, DAVIS WRIGHT TREMAINE. PRIV. & SEC. L. BLOG (June 16, 2020), https://perma.cc/RPW4-P9ML.

[181] *See, e.g.*, Brown v. Sirchie Acquisition Company, LLC, No. 1:16-CV-175-SCJ, 2017 WL 4082690, at *5-6 (S.D. Ga. Feb. 17, 2017).

unfair and deceptive practices under FTC Act 5(a).[182] The same action that makes such consent legitimate (disclosure) also reinforces trust and appropriate use in awareness of the possible errors. It is crucial for people to understand that, while immunity passports can be immensely valuable in terms of their informativeness, holding an immunity passport does not mean one is immune to the virus with a 100% probability (so some minimal precautions are warranted) and that someone lacking the immunity passport is not certain to be vulnerable to the virus (so they should not be categorically deprived of engaging in low-risk activities).

A difference between testing kit manufacturing and containment apps is that, in the latter, false positives depend on social behavior. For example, a contact tracing app will have more false positives for an individual if she takes safety measures such as wearing a mask, staying distanced, and being outdoors. This social behavior is also partly determined by government restrictions and recommendations. Therefore, no app developer can know in advance the percentage of false positives that will take place. Adequate disclosure, instead, can be achieved by indicating that the app may produce false positives and explaining what the rate of false positives depends on.

Liability also relates to the toggling of false positives and false negatives to minimize the latter issue discussed above. One way to arrive at such toggling of error rates is through private law, by developing no-fault compensation for false negatives for immunity passports. That is, if someone who was erroneously certified as immune by the app contracted the virus, they, and the people to whom they transmitted the virus, could have a claim against app developers. This measure can be achieved by drawing parallels with no-fault injury compensation regimes for vaccination.[183] The vaccination compensation regime aims to reduce error by internalizing externalities from vaccine injury and, indirectly, to increase confidence in vaccines.[184] Both of these policy aims arguably exist for immunity

---

[182] 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

[183] *See* Sam Halabi et al., *No-Fault Compensation for Vaccine Injury – The Other Side of Equitable Access to Covid-19 Vaccines*, 383 NEW ENG. J. MED. at 2 (2020) (arguing in favor of "leveraging two existing no-fault vaccine-injury regimens and constructing a third regime under COVAX's authority").

[184] Katharine Browne, *Vaccine Injury Compensation and the Common Good*, IMPACT ETHICS (May 13, 2016), https://perma.cc/TD9W-N4J6 (noting that Canada and Russia are the only G8 countries that lack national vaccine injury compensation programs); *Vaccine Injury Compensation Programmes*, WHO, https://perma.cc/ZDF6-73UQ (last visited Jan. 30, 2021) (recognizing no-fault vaccine injury compensation programmes as a measure to maintain confidence in vaccination efforts).

passports. In a no-fault regime, all that would be required would be to prove that the vaccine caused the injury. Usually, causation is a major hurdle to no-fault liability. But the internal use of immunity passports to exempt people from public health regulations is less likely to have that problem given that, but for a false negative, the person would have had to comply with those public health restrictions and they would have reduced his or her probability of contagion.[185]

C. Magnifying Inequalities

1. Over-surveillance, Stigma, and the HIV Epidemic

Another problem with inaccuracy is that algorithmic error is rarely distributed evenly.[186] As with many other systems, inaccuracy for containment apps is distributed in such a way that is likely to disproportionately harm the most vulnerable. This happens in two discrete ways. The first is with groups that are over-surveilled. The second is with groups that are left out.

The first form of magnifying inequality is selective over-surveillance. Contact tracing is most useful for the most vulnerable.[187] Among them are the economically vulnerable. Construction workers, delivery people, domestic workers, cashiers, bus drivers, and taxi or Uber drivers constantly come into contact with customers or each other in doing their jobs. Those who have a job where they are in contact with many others are precisely those who are important to trace and notify of potential exposure. Many of them, although not all, are classified as essential workers under state orders or directives.[188]

These groups benefit from the apps more. But greater proximity to others increases the likelihood that a contact tracing app alerts them of exposure even

---

[185] *See* Ignacio N. Cofone, *The Limits of Probabilistic Causality in Law*, 15 GLOB. JURIST 29, 54 (2015) (explaining the appropriate scope of probabilistic causality in tort law).

[186] Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1406 (2019) (discussing algorithmic bias and how it leads to discrimination).

[187] *See* Anne Andermann, *Outbreaks in the Age of Syndemics: New Insights for Improving Indigenous Health* 43 CAN. CMTY. DISEASE REP. 125, 126 (2017) ("Those who live in degraded physical and social environments are at greater risk of contracting, propagating and even dying from communicable diseases.").

[188] *COVID-19: Essential Workers in the States*, NAT'L CONF. STATE LEGIS. (Jan. 11, 2021), https://perma.cc/6W5Z-ZDSY (providing sector-specific information indicating that 23 states have developed lists under states' essential workers orders, that 20 states have referred to the cited agency's federal guidelines, and that the remaining 7 states have done neither); CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, GUIDANCE ON THE ESSENTIAL CRITICAL INFRASTRUCTURE WORKFORCE (2020), https://perma.cc/M4DX-Q5RA.

when safety measures are taken to keep the real risk low.[189] As a result, those who do not have a job that can be done from their homes are more likely to show a positive result on a contact tracing app. They are thus more likely to bear the economic and psychological harms of false positives. For app-based immunity passports, they would face an increased risk of being infected for having the mistaken confidence of being immune.

Using a containment app may also be less of a meaningful choice for them than it is for an average citizen if their employers or clients request that they use it.[190] At the same time, if positive results lead them to face negative outcomes at work (for example by having to take time off after receiving a positive alert), then the app amplifies problems of economic inequality. Their situation pairs error distribution with the consent element discussed above. This fact exemplifies the pattern that marginalized communities disproportionately experience surveillance and its accompanying risks.[191]

Contracting COVID-19 may carry social stigma that is unlikely to dissipate. When receiving an alert, people can draw correct or incorrect inferences to place blame on who may have exposed them.[192] The ease of inference depends partly on a contact tracing app's design. If alerts upon possible exposure are immediate, it may be easy to determine the identity of the infected person with whom one was in proximity. If alerts accumulate, with the person being alerted of collected possible exposures after a given period, the ease of inference and the possibility of assigning blame decrease. A number of these apps, for example, send notifications once a day.

The HIV epidemic across the United States provides informative experiences about the stigma of disease and the harm it produces. COVID-19 is the one of the few diseases besides HIV whose potential transmission has been criminalized in

---

[189] *See* discussion *supra* Part IV.A.

[190] *See supra* text accompanying note 97.

[191] Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. L. REV. 53, 67-74 (2017) (providing empirical data demonstrating the increased vulnerability of low-income Internet users to surveillance); Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1678 (2017) ("[P]erformative privacy helps highlight the disparate burden of surveillance on marginalized communities and identifies a collective form of political resistance.").

[192] Sara L.M. Davis, *Contact Tracing Apps: Extra Risks for Women and Marginalized Groups*, HEALTH & HUM. RTS. J. (Apr. 29, 2020), https://perma.cc/P555-ZQ6J (adding that such inferences have led individuals in South Korea to be accused of infidelity, sex work, and more).

the last 100 years.[193] Researchers and activists have warned against criminalizing risk of COVID-19 transmission based on the experience with HIV,[194] where criminalization has not helped containment and has further marginalized groups such as sex workers and LGBTQ people.[195] But a number of jurisdictions have criminalized the risk of COVID-19 transmission, either directly or indirectly by criminalizing breaking quarantine—in both cases contributing to stigma. Regarding indirect criminalization, Wisconsin's emergency order determines that a "violation or obstruction of this Order is punishable by up to 30 days imprisonment, or up to $250 fine, or both,"[196] and North Carolina's Mecklenburg Country issued a joint proclamation declaring that any person who violated it would be guilty of a Class 2 misdemeanor.[197]

Regarding direct criminalization, the Department of Justice indicated that, because COVID-19 is considered to meet the statutory definition of a biological agent, those who purposefully expose and infect others could be prosecuted under federal terrorism statutes.[198] Shortly after, people were charged with

---

[193] *See* discussion *supra* notes 92–95 and accompanying text. *See generally* EVAN LIEBERMAN, BOUNDARIES OF CONTAGION: HOW ETHNIC POLITICS HAVE SHAPED GOVERNMENT RESPONSES TO AIDS (2009) (discussing HIV criminalization in the context of risk and social competition).

[194] Nina Sun & Livio Zilli, *COVID-19 Symposium: The Use of Criminal Sanctions in COVID-19 Responses – Exposure and Transmission, Part I*, OPINIOJURIS (Mar. 4, 2020), https://perma.cc/9RJH-L75R (referring to COVID-19-related criminalization as "an alarming trend"); UNAIDS 2020, RIGHTS IN THE TIME OF COVID-19: LESSONS FROM HIV FOR AN EFFECTIVE, COMMUNITY-LED RESPONSE 9 (Mar. 20, 2020), https://perma.cc/YW6U-2WGN (holding that using criminal law to regulate COVID-19-related behavior is a "severe and drastic approach" that can "further stigmatize people who have the virus, dissuade people from getting tested and destroy trust between the government and communities.").

[195] Kyle Kirkup, *The Gross Indecency of Criminalizing HIV Non-Disclosure*, 70 TORONTO L.J. 263, 273–76 (2020) (noting queer men were most blamed for the spread of HIV); Kim Shayo Buchanan, *When Is HIV a Crime: Sexuality, Gender and Consent*, 99 MINN. L. REV. 1231, 1241–48 (2014) (explaining why empirical studies demonstrate that criminal laws are unlikely to reduce HIV transmission).

[196] Emergency Order #12, Dep't of Health Servs. (Wis. Mar. 24, 2020), https://perma.cc/F9AB-5RYT.

[197] COVID-19 Stay at Home Ordinance (Mecklenburg Cty., N.C. 2020), https://perma.cc/H65T-XJCM.

[198] Memorandum from the Deputy Att'y Gen. to All Heads of L. Enf't Components, Heads of Litigating Div., and U.S. Att'ys (Mar. 24, 2020), https://perma.cc/U5AC-HXBL; *see also* Paul LeBlanc, *People Intentionally Spreading Coronavirus Could Be Charged with Terrorism, DOJ Says*, CNN (last updated Mar. 25, 2020, 5:32 PM EDT), perma.cc/U99T-BXMT; Josh Gerstein, *Those Who Intentionally Spread Coronavirus Could Be Charged as Terrorists*, POLITICO (Mar. 24, 2020, 11:22PM EDT), https://perma.cc/6KX2-ZCBX.

terrorism-related crimes for coughing in Pennsylvania,[199] New Jersey,[200] and Missouri.[201] State crimes can also be applied. In Connecticut, for example, a doctor was arrested and charged with breach of peace for allegedly coughing and hugging coworkers.[202] And this tendency is by no means exclusive of the United States. Abroad, jurisdictions that similarly criminalized COVID-19 transmission or breaking quarantine include Argentina,[203] Bolivia,[204] Hong Kong,[205] Italy,[206] Russia,[207] Saudi Arabia,[208] Sudan,[209] South Africa,[210] United Arab Emirates,[211]

---

[199] *Pennsylvania Man Faces Charges for Deliberately Coughing near Elderly Man Who Was Wearing Medical Face Mask*, FOX 8 (Mar. 24, 2020, 10:19 AM EDT) https://perma.cc/J3X9-5LX9.

[200] *Coronavirus Latest: Men from New Jersey, Pennsylvania Charged After 'Purposely Coughing' on People, Saying They Were Infected, Prosecutors Say*, CBS PHILLY, (Mar. 24, 2020, 8:05 PM), https://perma.cc/GDJ8-RCEA.

[201] Minyvonne Burke, *Missouri Man Charged With Licking Items at Walmart to Mock Coronavirus Fears*, NBC NEWS (Mar. 25, 2020, 1 :34 PM PDT), https://perma.cc/6B57-2GQR.

[202] Sarah Al-Arshani, *A Connecticut Doctor Has Been Charged After Authorities Said He Deliberately Coughed on His Coworkers*, BUS. INSIDER (Mar. 27, 2020, 6:02 PM), https://perma.cc/Z75K-6P6T.

[203] Decreto Presidencial 260/20, DECNU-2020-260-APN-PTE; Decreto Presidencial DNU 297/20, DECNU-2020-297-APN-PTE (stating that arts. 205 & 239 of the Criminal Code are applicable to those who fail to comply with the measures established in them).

[204] Decreto Supremo No. 4200, Jeanine Áñez Chávez, Presidenta Constitucional del Estado Plurinacional de Bolivia.

[205] Huang et al., *supra* note 3 (explaining that quarantine violators in Hong Kong face up to six months in prison and a $3,200 fine).

[206] D.P.C.M. n. 59/2020, G.U. Mar. 8, 2020 (It.); D.P.C.M. n.62/2020, G.U. Mar. 9, 2020 (It.); Art. 650 C.p (It.).

[207] Federal'nyĭ zakon No. 100-FZ O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i stat'i 31 i 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii [Federal Law No. 100-FZ on the Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation], Apr. 1, 2020 (Rus.).

[208] Samaro, *supra* note 9 (explaining that attempts to remove the assigned bracelet are punishable by up to two years in prison and a fine of up to $53,268).

[209] Emergency Order No. 1 of 2020 Declaring a Public Health Emergency (Sudan) (the order criminalizes, *inter alia*, non-compliance with lockdown measures and failing to maintain physical distancing, non-compliance with requested medical examination, and disseminating incorrect information regarding the pandemic); *see also 'Intentional Murder': Careless COVID-19 Spreaders in Italy Could Face Homicide Charges*, NATIONAL POST (Mar. 12, 2020), https://perma.cc/GF87-89K8.

[210] Disaster Management Act 43107 of 2020 (S. Afr.); S Abdool Karim, *Criminalisation Of Transmission Of SARS-Cov-2: A Potential Challenge to Controlling The Outbreak in South Africa*, 110 S. AFR. MED. J. 458, 458 (2020).

[211] Federal Law No. 14 of 2014 to Combat Communicable Diseases (U.A.E.); *see also* Ali Al Shouk, *Coronavirus: Quarantine Violators in UAE Face up to Five Years in Jail*, GULF NEWS (Mar. 20, 2020, 4:05 PM), https://perma.cc/MF65-BYD4.

China's Hubei province,[212] and Canada's Ontario province.[213] Criminal coercion worsens already existing stigma and undermines trust in containment apps, which rely on cooperation.[214]

Criminalization is not necessary for stigma and social pressure to exist. Collecting and publishing aggregated location data about COVID-19 outbreaks intensifies both. Outbreaks linked to certain communities, religious groups, or neighborhoods, would likely create or intensify stigma towards them, like they did during the HIV epidemic.[215] This makes decentralized contact tracing apps that do not gather location (top left quadrant on table 1) less risky than those that do—at least in terms of enhancing discrimination.

This is important in a social context where COVID-19 has already intensified anti-Asian xenophobia and racism worldwide, as reported by Human Rights Watch.[216] The Anti-Defamation League released a list of racist attacks and harassment against Asian people occurring in the US on an almost daily basis,[217] including situations of (unilateral) physical violence.[218]

---

[212] Ping An Hubei, *Notice of Hubei Provincial Public Security Department: Severely Crack Down On Six Types of Medical Crimes*, WEIXIN, (Jan. 29, 2020), https://perma.cc/63C6-UF7B; Alex Lin, *Carriers of the Wuhan [sic] Coronavirus Face Criminal Charges if They Knowingly Infect Others in Hubei*, CNN (Jan. 30, 2020, 12:33 AM ET), https://perma.cc/LA2M-S4BV.

[213] Emergency Management and Civil Protection Act, R.S.O. 1990, c. E.9, s. 7.0.11(1)(a) (establishing punishment for breaching restrictions on gatherings with a fine of up to $100,000 and up to a year's imprisonment).

[214] *See* Lawrence Gostin & James Hodge, *US Emergency Legal Responses to Novel Coronavirus: Balancing Public Health and Civil Liberties*, 323 JAMA 1131, 1131–32 (2020) ("Coercive [public health] measures could be counterproductive and erode public trust and cooperation."); Matthew M. Kavanagh & Renu Singh, *Democracy, Capacity, and Coercion in Pandemic Response: COVID-19 in Comparative Political Perspective*, 45 J. HEALTH POL. POL'Y & L. 997 (2020) (arguing against coercive measures to contain COVID-19).

[215] Kirkup, *supra* note 195, at 273 ("[W]hen the epidemic first emerged in the 1980s, the condition came to be synonymous with the purportedly promiscuous, deviant, pathological lives of queer men."); Buchanan, *supra* note 195, at 1294 ("Gendered, racial, and homophobic bias are notorious throughout the enforcement of criminal law, from drug possession through rape and the death penalty. The role of such biases in HIV criminalization may run deeper, shaping . . . perceptions about whether, when, and why HIV should be treated as a crime.").

[216] COVID-19 FUELING ANTI-ASIAN RACISM AND XENOPHOBIA WORLDWIDE: NATIONAL ACTION PLANS NEEDED TO COUNTER INTOLERANCE, HUM. RTS. WATCH (May 12, 2020, 3:19 PM EDT), https://perma.cc/NWU8-DKHA; *Zaia Sui Cinesi: «Li Abbiamo Visti Tutti Mangiare I Topi Vivi»*, FLASHES (Feb. 28, 2020, 4:45 PM) https://perma.cc/RPH9-PQTF (highlighting that the Governor of Veneto, Italy told journalists that Chinese people have relatively bad hygiene, don't wash their hands, don't shower, and eat mice alive).

[217] *E.g.*, *Reports of Anti-Asian Assaults, Harassment and Hate Crimes Rise as Coronavirus Spreads*, ANTI-DEFAMATION LEAGUE (June 18, 2020), https://perma.cc/J34Q-X2ML (citing local reporting).

[218] *'Where's Your (Expletive) Mask?': Asian Woman Attacked in Manhattan Hate Crime*, ABC7 (Mar. 11, 2020), https://perma.cc/9TFL-3HNM (describing an event where an Asian woman in Manhattan, New York, was punched in the face, chin and shoulder and was taken to the

Containment apps have the potential to make this worse. A Korean doctor, for example, reported that some of their patients were more afraid of being blamed than they were of death.[219] Human rights experts, similarly, were reportedly alarmed by naming and shaming in public of those who has contracted COVID-19 in Cambodia, leading to overt discrimination.[220] Fear of stigmatization can also discourage cooperating with contact tracing, including app use. So too can fear of increased visibility when it leads to disadvantages, for example, for undocumented immigrants.

2. Furthering Marginalization

The second form of magnifying inequality exists at the other end of the spectrum, with the vulnerable that the apps exclude. Those who are more vulnerable to the virus because of their living conditions are also less likely to own a smartphone new enough to support these apps.[221] The elderly living in care facilities, the homeless, migrants, refugees, and prisoners, all live in conditions that make them more likely to contract the virus; meanwhile, they lack the means that will also give them access to a device that can support an app to detect or report transmission or one to certify that they are immune. If immunity passports are used for exceptions to quarantine requirements, they would be excluded from a system of privileges and exceptions.[222]

Because this set of vulnerable groups will receive less surveillance, they will receive less accuracy in terms of error rates—and, with it, less power. New levels of digital divide often deepen existing inequalities.[223] This deepening of the

---

hospital with a possible dislocated jaw); Christina Capatides, *Bullies Attack Asian American Teen at School, Accusing Him of Having Coronavirus*, CBS NEWS (Feb. 14, 2020, 1:53 PM) https://perma.cc/EC78-MDUB (describing how a 16-year-old student in San Fernando Valley, California, was attacked in school by bullies who accused him of having COVID-19 because he is of Asian descent).

[219] Ramesh Raskar et al., *Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic*, ARXIV 1, 7 (2020).

[220] *Cambodia: UN Experts Alarmed By 'Naming and Shaming' of COVID Victims*, U.N. HUM. RTS. OFF. HIGH COMM'R (Dec. 11, 2020) https://perma.cc/5C9J-56XK.

[221] Cyphers & Gebhart, *supra* note 131 (adding that "even a proximity tracking system with near-universal adoption is going to miss millions of contacts each day" because phones can be turned off, left at home, etc.).

[222] FAQ, *supra* note 53 (recognizing the privileges and exceptions that holding an immunity passport bestows, including allowing one "to return to a normal life (work, school, sports, social interaction/activities, meeting at-risk groups)"); *see also* McLean & Davey-Attlee, *supra* note 61 (describing the privileges in Iceland and Hungary).

[223] *See* Sofia Ranchordás, *Connected but Still Excluded? Digital Exclusion Beyond Internet Access*,

digital divide along lines of vulnerability exists between people who use the app and entire communities that cannot.[224] Although the negative effects of oversurveillance discussed above may make being left out of the system sound desirable, it is not. First, because low accuracy may mean that they disproportionately suffer from the side effects of uneven surveillance in terms of stigma, piling on existing inequalities. Second, because to the extent that the public health response may rely on surveillance-produced data, for example by allocating doctors or resources depending on the number of reported positive results, these communities will be left out of such effort.

This reality extends to people in those communities who do have the app, as it may skew their responses to COVID-19 and their willingness to adopt other health measures. For instance, they will not receive a notification when they have come into contact with someone who is positive but does not have a contact tracing app. Therefore, they may not think that the disease is a significant problem in their neighborhood, or that they are at risk of contracting it. They may alter their behavior by no longer wearing a mask, distancing, etc. More broadly, this may lead them not to take the disease as seriously as they should—or as it is in their best interest to.

This issue leads to an irony that has been pointed out for other technologies.[225] Vulnerable groups that receive less surveillance from containment apps receive less accuracy and are more likely to suffer from the apps' side effects in terms of discrimination. This problem is similar to the one racialized individuals experience with facial recognition, being identified with less accuracy than non-racialized individuals.[226] Although this surveillance avoidance may sound advantageous, it leads these groups to face difficulties at workplaces that rely on

---

CAMBRIDGE HANDBOOK LIFE SCI., INFORMATIVE TECHN. & HUM. RTS. (M Ienca et al., eds., 2021) (discussing the relationship between the digital divide and the deepening of existing inequalities).

[224] Teresa Scassa et al., *Privacy, Ethics, and Contact-Tracing Apps*, *in* VULNERABLE: THE LAW, POLICY AND ETHICS OF COVID-19 249, 261 (Colleen M. Flood et al., eds., 2020) (recognizing that COVID-19 responses which seem even-handed on their face may still offend a differentiated understanding of equality).

[225] *See, e.g.*, Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://perma.cc/MSC4-4TL9 (noting that facial-recognition algorithms perpetuate racial bias because they are significantly more accurate when identifying white versus non-white faces).

[226] Tellingly, facial recognition startups have been among the first to pitch immunity passport apps to governments. *See* Thomas Brewster, *Facial Recognition Firms Pitch Covid-19 'Immunity Passports' for America and Britain*, FORBES (May 20, 2020, 8:58 AM PDT), https://perma.cc/4R93-8KZZ.

facial recognition for identification and it leads them to face an increased risk of wrongful arrest.[227]

Because of this accuracy problem, allocating public health or medical resources based on mapping those who marked themselves positive for COVID-19 on contact tracing apps, or mapping populations with fewer people marked as immune on immunity passports, will ignore a sizable portion of the population (many of whom are highly vulnerable). It will thereby skew benefits towards younger and wealthier users who are more likely to use apps but less likely to suffer severe health problems if infected. Contact tracing apps with a centralized component, as mentioned above, can provide useful public health information on spread. But such information will be skewed by the biases and characteristics of the dataset, which will be unrepresentative of the general population.

As Sarah Davis puts it:

> "Health data is not neutral: it is embedded in political contexts, can be shaped by politics, and its collection and use in decision-making has life-or-death effects. While we are all desperate for solutions to the COVID-19 crisis, history, including decades of the HIV response, has shown that addressing epidemics requires thoughtful consideration for how the rights of those most marginalized undermines their participation in the programs and strategies devised for the health of all."[228]

3. Immunity Passports' Layers of Privilege

This second inequality problem is the biggest concern for immunity passport apps. Immunity passports could worsen existing inequalities. The history of a previous epidemic in the United States–yellow fever–provides precedent for this. During much of the Nineteenth Century, people in Louisiana were divided

---

[227] Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33 (2020); Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 96–103 (Amba Kak, ed., 2020); Lindsey Barrett, *Ban Facial Recognition Technologies for Children – And for Everyone Else*, 26 B.U. J. SCI & TECH. L. 223, 247-59 (2020) (recognizing that children of color are at an especially high risk of being wrongfully accused of a crime due to facial recognition technology); Lisa Toohey et al., *Meeting the Access to Civil Justice Challenge: Digital Inclusion, Algorithmic Justice, and Human-Centred Design*, 19 MACQUARIE L.J. 133, 147–51 (2019) (recognizing the problem posed by facial recognition in the context of algorithmic bias); David Leslie, *Understanding Bias in Facial Recognition Technologies*, ALAN TURING INST., at 12–19 (2020) (discussing how facial recognition technology has perpetuated historical biases).

[228] Davis, *supra* note 192.

between those who had recovered from the fever and were thus immune (called "acclimated") and those who had not (called "unacclimated").[229] The acclimated carried an immunity certification and the unacclimated faced restrictions for obtaining work, living in certain neighborhoods, and marrying.[230] Immunity became a type of privilege that corresponded with having the tools to survive the disease, and divided citizens along race and class.[231]

As health ethicists have noted, "there will indeed be two different types of citizens."[232] The purpose of the passports is to give those who are certified as immune "a range of opportunities that would be restricted for others, potentially across a wide range of domains."[233] The passports, in doing so, will create an added layer of privilege. First, they will bestow privilege on those with access to the app itself. Second, they will do so on those who have access to sources of immunity. This has led some to believe that:

> "In a world where immunity passports are the norm and systemic racism abounds, only those lucky enough to have survived COVID-19, privileged enough to have access to immunity testing, white enough to avoid police scrutiny, and rich enough to own a smartphone to display their status on demand would be able to return to work, social activities, and travel. The rest would not."[234]

Regarding the first layer of added privilege (those with access to the app itself), all immunity passports face the problem that marginalized groups such as the homeless and the elderly are less likely to own a smartphone that can support the apps being developed. Their benefits would be available only to those with a smartphone that can hold them—or, in the case of printable ones like the Digital

---

[229] Kathryn Olivarius, *Immunity, Capital, and Power in Antebellum New Orleans*, 124 AM. HIST. REV. 425, 425–55 (2019).
[230] *Id.*
[231] *Id.*; *see also* Natalie Kofle & Francoise Baylis, Comment, *Ten Reasons Why Immunity Passports Are a Bad Idea*, 581 NATURE 379 (2020) (tracing the analogy with COVID-19).
[232] Iñigo de Miguel Beriain & Jon Rueda, *Immunity Passports, Fundamental Rights and Public Health Hazards: A Reply to Brown et al*, 46 J. MED. ETHICS 660, 661 (2020).
[233] Daniel Weinstock & Vardit Ravitsky, *Should Immunity Licences Be an Ingredient in Our Policy Response to COVID-19?*, *in* VULNERABLE: THE LAW, POLICY AND ETHICS OF COVID-19 277, 282 (Colleen M. Flood et al., eds., 2020).
[234] Natalie Kofler & Françoise Baylis, *Immunity Passports – Reopening the Economy and Repackaging Racism*, J. MED. ETHICS BLOG (Jul. 1 2020), https://perma.cc/NV6B-DG2G.

Green pass, with access to a printer. Providing people with a non-digital alternative, such as a card with a QR code for scanning, reduces this problem.

Regarding the second layer of added privilege (those who have access to certified sources of immunity), immunity passports vary. There are three alternatives affecting the extent to which they extend systemic inequality, depending on what kind of data they are based on.

The first alternative is an immunity passport app that only recognizes vaccination data, which may be the most popular alternative abroad.[235] This option traces inequality only to the extent the vaccine distribution does. This enhancement of inequality may not be significant if low-income groups have no-cost access to vaccinations, but it would otherwise. Their main equity risk is that access could follow patterns of medical discrimination where, for example, Black individuals are less likely to receive vaccines.[236] If racialized groups are vaccinated against COVID-19 less, then they would be less likely to receive an immunity passport and, thus, be further marginalized and excluded from social and commercial activities.

The second alternative is a passport that logs data from vaccine data and antibodies. This can be done either through serology tests, which detect antibody responses to COVID-19, or through data showing that one was infected with the virus and recovered. Incorporating serology tests would turn, to a large extent, into a passport mostly useful to those who can afford rapid private testing, building on inequitable access to antibody testing. It would be the most problematic option from an equality perspective. According to Human Rights Watch, incorporating recovery data may problematically create perverse incentives for people who cannot afford other means of certification to infect themselves—hoping to then recover and have certified immunity.[237] This problem occurred during the AIDS epidemic when individuals sought infection to release themselves from the restrictions of avoiding the virus; and some fear

---

[235] *See, e.g.*, *supra* notes 93-95 and accompanying text on apps from Bahrain, Brunei, Estonia, Greece, and Saudi Arabia.

[236] Dan Royles, *Years of Medical Abuse Make Black Americans Less Likely to Trust the Coronavirus Vaccine*, WASH. POST (Dec. 15, 2020, 3:00 AM PST), https://perma.cc/6P89-BZRL; April Dembosky, *It's Not Tuskegee. Current Medical Racism Fuels Black Americans' Vaccine Hesitancy*, L.A. TIMES (Mar. 25, 2021, 12:10 PM PT), https://perma.cc/N8XQ-KLEW.

[237] Kenneth Roth & Annie Sparrow, *Should People Without Coronavirus Antibodies Be Second-Class Citizens?*, N.Y. TIMES (Apr. 28, 2020), https://perma.cc/G2UT-6SD9 (arguing that we should "stop and think before we start issuing 'immunity passports'"); *see also* McLean & Davey-Attlee, *supra* note 61 ("[A]ll of a sudden, you'd see people not wearing masks, not respecting social distancing, because they want to get COVID.").

that COVID-19 may encourage similar behavior.[238] This problem would be worsened if immunity passports loosen restrictions.[239] The EU Digital Green Certificate faces this problem as, in addition to vaccine and PCR data, it recognizes certificates for persons who recovered from COVID-19.

The third alternative is a passport that, in addition to vaccine data, also accepts data from negative PCR tests within a certain window of time. New York's Excelsior Pass takes this model, accepting data from vaccines, negative PCR tests, and antigen tests (so-called rapid tests),[240] as does Malaysia's and Singapore's Immunitee. These apps are in between the two prior alternatives in terms of inequality, tracking contact tracing apps' unequal distribution. But, if governments provide free access to PCR testing, they can avoid adding the layer of inequality of those with access to privatized medicine.

Here a reader may wonder, what if immunity passports were used in a more restricted manner, only to police international transit? They would present the same two problems, at a smaller scale. If used to condition entry to the country, immunity passports would negatively affect immigrants and refugees. Many countries will not have widely distributed vaccines until years after the United States. If the United States required an immunity passport based on vaccination to enter the country or immigrate, developing countries receiving insufficient vaccines would be unable to provide this certification to their citizens. The apps would add an additional layer of inequality in preventing immigration that would be borne by the poor.

Yellow fever passports (small yellow paper booklets) are still used in parts of Africa and South America to police transit between countries.[241] Paper vaccine

---

[238] Alexis Hancock & Karen Gullo, *Immunity Passports Are a Threat to Our Privacy and Information Security*, ELEC. FRONTIER FOUND. (May 28, 2020), https://perma.cc/H2UZ-254J ("No one should have to expose themselves to a potentially deadly disease with no cure to find work."); Teck Chuan Voo et al., *Ethical Implementation of Immunity Passports During the COVID-19 Pandemic*, 222 J. INFECTIOUS DIS. 715, 716 ("The ability to return to work sooner may provide perverse incentives to deliberately increase one's SARS-CoV-2 exposure."); Sarah Boseley, *Covid-Status Certificates Could Lead to Deliberate Infections, Scientists Warn*, GUARDIAN (Apr. 11, 2021), https://perma.cc/HSV8-FYQW.

[239] *See generally* Daniel Hemel & Anup Malani, *Immunity Passports and Moral Hazard*, (U. Chi. Coase-Sandor Inst. for L. & Econ. Research Paper No. 905, 2020), https://perma.cc/2R6R-U5D6 (discussing strategic self-infection as a moral hazard problem).

[240] Kent Sepkowitz, *Why the First State Vaccine Pass Isn't Ready for Prime Time,* CNN (Mar. 29, 2021, 9:54 PM ET), https://perma.cc/2KYD-DGCM.

[241] Mark D. Gershman & J. Erin Staples, *Yellow Book - Travel-Related Infectious Diseases - Yellow Fever*, CDC, https://perma.cc/V5SR-VGKK (listing Angola, Benin, Burkina Faso, Burundi,

certificates such as this one can be stolen or falsified.[242] Although immunity passports aim to resolve these two problems, they contain an enhanced version of their inequality problem, as the use of yellow fever passports in Nineteenth Century Louisiana illustrates. Some may consider that exacerbation of inequality to be acceptable for loosening public health restrictions for those who do not need them. The next Part addresses this question.

V. HOW CONTAINMENT APPS FIT IN BALANCING PUBLIC HEALTH RESTRICTIONS

A. Identifying the Surveillance Tradeoff

1. Surveillance Is Persistent

Parts III and IV explained that the health information collected by containment apps cannot be fully anonymous and cannot rely on consent to prevent harm—and there are measures to de-identify more securely and improve consent. This is important because such data may produce harms like income loss, deportation, or detrimental effects on healthcare and insurance. Such data is prone to producing stigma, and it combines in problematic ways with asymmetric rates of error for marginalized groups. These data can be combined problematically with other actions, such as criminal sanctions for COVID-19 risk of transmission as implemented in some countries.

A key factor is for how long these measures' surveillance will continue to exist. Once surveillance takes place, it rarely fades when those supporting it expect—and when it should. As Human Rights Watch has put it: "The long history of emergency measures shows that when surveillance is introduced, it usually goes too far, fails to meet its objectives, and once approved, often outlasts its justification. Mobile tracking programs intended to be temporary measures until the pandemic is under control and a vaccine is available may become permanent features of an expanded surveillance regime."[243]

Cameroon, Central African Republic, Republic of the Congo, Côte d'Ivoire, Democratic Republic of the Congo, French Guiana, Gabon, Ghana, Guinea-Bissau, Mali, Niger, Nigeria, Sierra Leone, South Sudan, Togo, and Uganda, as well as other countries that require it for travelers arriving from high-risk countries).

[242] Patricia Schlagenhauf et al., *Variants, Vaccines and Vaccination Passports: Challenges and Chances for Travel Medicine in 2021*, TRAVEL MED. & INFECTIOUS DIS., Mar.-Apr. 2021, at 1, 2.

[243] *Covid-19 Apps Pose Serious Human Rights Risks*, HUM. RTS. WATCH (May 13, 2020, 12:01 AM EDT), https://perma.cc/6NGE-S7YU.

Anti-terrorism surveillance measures that were created as a response to the September 11 attacks and continue to exist today are a clear example of this tendency and this concern.[244] The Section 215 metadata program of the Patriot Act (then USA Freedom Act), which engaged in bulk collection of communications metadata to aid in combating terrorism, has been repeatedly extended.[245] It has been indicated as an example that, once surveillance authorities are granted, they are difficult to forego by the agencies empowered with them, even when it is demonstrated that they are no longer necessary—and even ineffective, costly, and of dubious legitimacy.[246]

Therefore, it is imperative to guarantee that containment apps' surveillance will sunset when the pandemic is under control, with a clear condition set in advance such as when vaccines are widely distributed or the WHO declares that the pandemic ended. The surveillance infrastructure developed for containing COVID-19 should not be extended for tracking milder health issues in the future without a separate assessment—as it easily could—or to engage in location or proximity surveillance for other purposes. While the roadmap presented here can be used for future containment surveillance measures, these measures should be specific to each particular crisis and not extend to normal times.

However, as of today, no state governments have provided such guarantee. Abroad, very few countries have issued clear sunset clauses for their contact tracing apps and it is unlikely that many will do so for immunity passports.[247]

---

[244] *See, e.g.*, Casey Ross, *After 9/11, We Gave Up Privacy for Security. Will We Make the Same Trade-Off After Covid-19?*, STAT (Apr. 8, 2020), https://perma.cc/X9X8-96KB (tracing the analogy between 9/11 surveillance and COVID-19 surveillance and citing Glen Cohen who said that "We tend to accept what we live in as far as what privacy is, and once we're there, the status quo has a lot of power over us").

[245] *See* Susan Landau & Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?*, 11 HARV. NAT'L SEC. J. 308, 321-40 (2020); Asaf Lubin, "*We Only Spy on Foreigners*": *The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L L. 502, 511-14 (2017) (describing programs of bulk interception, collection, and data mining on citizens).

[246] Landau & Lubin, *supra note 245*, at 321-40.

[247] Australia passed legislation requiring all data gathered through their contact tracing app be deleted once the pandemic is considered to be finished. *See* Privacy Amendment (Public Health Contact Information) Act 2020 (Cth) div. 3 s 94L (Austl.) (preventing at § 94K data collected through its contact tracing app from being stored for more than 21 days). The French government has informally guaranteed that it will phase out its app post-pandemic. *Tousanticovid : L'application Qui Alerte les Contacts d'un Malade du Covid-19*, Republique Francaise Service Public (Feb 3, 2021), https://perma.cc/27M9-6MT7 ("L'application « TousAntiCovid » est temporaire, elle n'a pas vocation à perdurer après la crise sanitaire.",

Moreover, it can be hard to believe the truthfulness of such sunset clauses. Promises that surveillance respond to a concrete crisis and it will be phased out as soon as the crisis is over, like the Patriot Act shows, are often empty.

2. Surveillance Versus What?

Data protection authorities from around the world have emphasized that national and state governments rolling out containment apps must apply the principle of proportionality to any measures that may impact people's privacy.[248] If any containment apps are challenged in the judiciary, courts would have to apply balancing tests, which weigh the competing rights in play.[249] There is little guidance, however, as to how proportionality and balancing tests should proceed.[250]

A key aspect of such tests often overlooked in this context is what rights or interests ought to be balanced. Public health and pandemic containment would win any balancing exercise. Senators Bob Menendez, Cory Booker, and Richard Blumenthal together with then-Senator and now-Vice-President Kamala Harris, for example, wrote in an early letter to Apple that "Americans should not have to trade their privacy at the expense of public health needs."[251] But the appropriate balancing exercise is not, as is often discussed, between privacy and public health.[252] The tradeoff, instead, is between privacy and the measures for containment that would otherwise be taken. More concretely, it is between

---

which translates to "the TousAntiCovid application is temporary; it is not meant to last after the health crisis is finished."). The European Union announced that the Digital Green Certificate will be suspended once the WHO considers the pandemic has ended, but adding that if a similar public health emergency arises the system could be reactivated. European Commission Press Release IP/21/1181, European Commission, Coronavirus: Commission proposes a Digital Green Certificate, (Mar. 17, 2021).

[248] *E.g.*, *Commissioner Issues Guidance on Privacy and the COVID-19 Outbreak*, OFF. PRIVACY COMM'R CAN., (Mar. 20, 2020), https://perma.cc/KEX2-BLUQ.

[249] *See* Patrick McFadden, *The Balancing Test*, 29 B.C. L. REV. 585, 603-22 (1988) (explaining the balancing test and its popularity).

[250] H Gunnarsdóttir et al., *Applying the Proportionality Principle to COVID-19 Antibody Testing*, 7 J. L. & BIOSC. 58 (2020) (calling for proportionality and balancing assessments in the context of COVID-19 and proposing one for antibody testing).

[251] Letter from Sen. Robert Menendez et al. to Tim Cook (Apr. 3, 2020) https://perma.cc/8AM9-JPQC.

[252] *See, e.g.*, Karen Hao, *Coronavirus is Forcing a Trade-Off Between Privacy and Public Health*, MIT TECH. REV. (Mar. 24, 2020), https://perma.cc/L9MC-SCKY (presenting the tradeoff of contact tracing apps as one between privacy and public health and stating that "[t]he trade-offs that EU regulators are facing mirror the tug-of-war between data privacy and public health that many governments and companies are now grappling with").

privacy and the economic development that avoiding such measures facilitates, people's mental health, and avoidance of corollaries of the quarantine such as an increase in domestic violence,[253] as well as lockdowns' perverse distributive effects.[254] This identification is consequential because the extent to which people are willing to give up freedoms such as privacy depends on what is at stake. When ambiguous objectives such as "public health" or "terrorism" are presented, it becomes more difficult to conduct a nuanced analysis.

The tradeoff is such partly because a well-enforced quarantine reduces the usefulness of any containment app—and, conversely, containment apps allow for more flexible quarantine measures.[255] Most of containment apps' benefits exist when governments relax (or altogether avoid) lockdown measures, allowing people to carry out their normal activities.[256] Moreover, using an app as an aid to quarantine people—as some countries did, as shown above—is ineffective because people can turn off GPS or Bluetooth to break quarantine or, in an act of obfuscation, leave their phone at home.[257]

The question, in other words, is not whether to pursue public health. The question is how to do it: whether to open businesses and have aggressive surveillance-enabled containment or to close businesses and keep people in their homes so that few contacts take place for as long as possible.[258] Of course, such a choice is not categorical but exists at the margins. As governments strive to

---

[253] Tanguay-Renaud et al., *supra* note 18, at 12 (arguing that balancing is between privacy and other Charter values such as security of the person and equality).

[254] Lockdown is more burdensome for marginalized populations. As François Tanguay-Renaud et al. explain, "Individuals who self-isolate in situations of poverty, precarious housing, mental health challenges, abusive relationships, or other vulnerabilities face challenges that affect their security of the person." *Id*. at 12.

[255] While this is true for both types of apps, contact tracing apps operate slightly differently from immunity passports in this regard because contact tracing's usefulness is correlated to the number of contacts, which depend directly on the lack of restrictions. Immunity passports, on the other hand, can serve a purpose in a scenario of heavy lockdown restrictions where there are selective releases for those considered immune.

[256] In a well-enforced quarantine, these apps would only be useful for doctors, delivery employees, and others that continue to carry out activities that place them in contact with others.

[257] *See generally* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015) (discussing acts of obfuscation and how they relate to enhancing privacy).

[258] *See* Lanzing, *supra* note 90, at 2 ("Moreover, 'health versus privacy' is a false contradiction. Health and privacy are not necessarily mutually exclusive."); Cattuto & Spina, *supra* note 90, at 233 ("It should first be observed that the introduction of a mobile phone app as a solution to implementing an effective form of contact tracing has been marred by incorrect assumptions and false dichotomies, the first and foremost being the one that accepts that there is a trade-off between the need to respect privacy/data protection and public health.").

distribute vaccines, the choice is not between entering another general lockdown or keeping everything open while implementing contact tracing. Rather, each choice about whether to open factories, stores, schools, and so on, is a choice between the costs of moving the dial of lockdown's economic impacts and the dial of containment surveillance.

From a balancing point of view, the strongest argument for being vigilant about intensifying containment surveillance is that a well-enforced quarantine alone could be less detrimental to other human rights than the surveillance mechanisms involved in most of these apps. The economic and psychological costs of a lockdown, however, lead many to conclude that apps ought to be rolled out despite their risks and lockdown measures ought to be relaxed. Whichever the decision is, it is important to do so understanding of the implications of the policy choice.

B. Proportionality and the Least Restrictive Means

1. Identifying the Least Restrictive Means

One of the cornerstone principles of public health ethics is that of the "least restrictive intervention."[259] The principle means that, in situations where restricting rights or freedoms may be needed, any measure should only be used after having attempted or considered less restrictive alternatives.[260]

The principle of applying the least restrictive measure among possible interventions informs evaluations of proportionality.[261] A public health emergency such as a pandemic should not be a justification for suspending rights when doing so is not necessary or proportionate to address the pandemic effectively.[262] Particularly, choosing the least restrictive measure to achieve any given aim is central to the proportionality analyses required for restricting rights

---

[259] *See* Ross D. Silverman, *Contact Tracing, Intrastate and Interstate Quarantine, and Isolation*, *in* ASSESSING LEGAL RESPONSES TO COVID-19 28, 30 (Scott Burris et al., eds., 2020); James Childress et al., *Public Health Ethics: Mapping the Terrain*, 30 J.L. MED. & ETHICS 170, 173 (2002) (discussing it as the "least infringement" principle).

[260] *See, e.g.*, Ross E. G. Upshur, *Principles for the Justification of Public Health Intervention*, 93 CAN. J. PUB HEALTH 101 (2002).

[261] *See* Nancy Kass, *An Ethics Framework for Public Health*, 91 AM. J. PUB. HEALTH 1776 (2001) (presenting the framework as one in which one should ask: is the measure proposed effective? Is there a benefit? Does the benefit outweigh the harms?).

[262] Gilad Abiri & Sebastian Guidi, *The Pandemic Constitution*, 59 COLUM. J. TRANSNAT'L L. (forthcoming 2021).

during an emergency under international human rights law.[263] At least at a policy level, human rights principles come into play due to the underlying inequality created by COVID-19 and the possibility that containment apps may exacerbate it.[264]

More broadly, as David Beatty argues: "Laws—indeed any act undertaken in the name or with the authorization (explicit or tacit) of the state—must respect a basic principle of proportionality in the way they deal with the different interests and values they affect."[265] Similarly, to comply with the WHO International Health Regulations (2005), public health measures must have a rationale, be non-discriminatory, consider human rights, and not be more restrictive than reasonable alternatives, [266] requirements that subsume a proportionality analysis.

Proportionality, in turn, is often part of balancing exercises in Constitutional Law for those evaluations that do not have categorical presumptions—as opposed to those of the First Amendment and Fourth Amendment.[267] The Court has used proportionality in balancing assessments, for example, in the Eighth Amendment,[268] the Due Process Clause,[269] the Takings

---

[263] *See* International Covenant on Civil and Political Rights art. 4, Dec. 16, 1966; U.N. Comm'n on Hum. Rts., *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Sept. 28, 1984, E/CN.4/1985/4 (providing authoritative guidance on human rights restrictions in cases of emergency). *See also* U.N. Hum. Rts. Comm., *Statement on Derogations from the Covenant in Connection with the COVID-19 Pandemic* (Apr. 30, 2020) (examining whether individual countries took disproportionate measures in their COVID-19 containment efforts).

[264] Alessandro Spadaro, *COVID-19: Testing the Limits of Human Rights*, 11 EUR. J. RISK REG. 317 (2020) (explaining that measures to contain the pandemic require a human rights law analysis because they can have a detrimental effect on the enjoyment of a number of human rights). *See also* discussion *supra* Part IV.C.

[265] DAVID M. BEATTY, THE ULTIMATE RULE OF LAW 160 (2004) (adding at 163 that "proportionality is an integral, indispensable part of every constitution that subordinates the system of government it creates to the rule of law").

[266] WHO, INTERNATIONAL HEALTH REGULATIONS (3d ed. 2016).

[267] Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1295–96, 1330–34 (2007) (adding that one problem regards "the difficulty of knowing in advance whether particular restrictions on protected rights would be either necessary or sufficient to forestall the threat."); David S. Law, *Generic Constitutional Law*, 89 MINN. L. REV. 652, 691–703 (2005) (characterizing proportionality in general and in several different legal jurisdictions).

[268] *See, e.g.*, Graham v. Florida, 560 U.S. 48, 59 (2010); Atkins v. Virginia, 536 U.S. 304 (2002); Roper v. Simmons, 543 U.S. 551 (2005); Miller v. Alabama, 132 S. Ct. 2455 (2012); United States v. Bajakajian, 524 U.S. 321 (1998).

[269] *See, e.g.*, State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 425-26 (2003); BMW of N. Am. v. Gore, 517 U.S. 559 (1996).

Clause,[270] the undue burden standard in abortion cases,[271] federalism,[272] and the Commerce Clause,[273] among others.[274] While recognizing proportionality does not necessarily mean that the judiciary should be involved in determining the best way to achieve balanced decision-making, it does mean that there are maxims of the Constitution that are relevant.[275] And these should be taken into account by the Executive and the Legislature when making policy decisions. These include the selection and rollout of something that this Article has shown to have enormous consequences for civil rights and liberties, and enormous public health utility in the context of a pandemic, such as containment apps.

2. Proportionality as a Policy Tool for Containment Apps

One way to implement the principle of least restrictive intervention in a proportionality analysis of a containment app is to build on the FTC's Fair Information Practice Principles (FIPPs). These principles are the basis of most privacy legislation in the United States.[276] The principles are notice (or awareness), choice (or consent), access (or participation), and integrity (or security).[277] A draft bill seemingly built on these principles, called the COVID-19 Consumer Data Protection Act of 2020, was introduced in Senate last May and ultimately did not pass.[278] The bill was meant "[t]o protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis."[279] While meant for

[270] *See, e.g.*, Koontz v. St. Johns River Water Mgmt. Dist., 570 U.S. 595, 596-97 (2013); Dolan v. City of Tigard, 512 U.S. 374, 391, 398 (1994).
[271] *See, e.g.*, Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 878 (1992).
[272] *See, e.g.*, City of Boerne v. Flores, 521 U.S. 507 (1997).
[273] Jud Mathews & Alec Stone Sweet, *All Things in Proportion? American Rights Review and the Problem of Balancing*, 60 EMORY L.J. 797, 814–24 (2011).
[274] Vicki C. Jackson, *Constitutional Law in the Age of Proportionality*, 96 YALE L.J. 943 (2015) (arguing for proportionality within balancing exercises).
[275] *Id*.
[276] They are the basis of federal legislation such as HIPAA, the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Cable Television Protection and Competition Act, and state legislation such as the CCPA. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) (discussing Europe's General Data Protection Regulation and the California Consumer Privacy Act in relation to principles for fair information processing).
[277] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7-14 (1998), https://perma.cc/F6LB-9XBV.
[278] S. 3663, 116th Cong. (as introduced in Senate on May 07, 2020).
[279] *Id.* at preamble.

contact tracing apps, nothing in the bill (or similar bills) would prevent it from being applied to all containment apps.[280]

Among other provisions, the bill would have delineated the meaning of de-identified information,[281] contained provisions on consent that included some mandates of transparency,[282] and a data accuracy provision aiming to reduce error rates.[283] While the bill would certainly not have solved all issues explained in this piece, it would have provided similar protection to that suggested by organizations such as the American Civil Liberties Union,[284] and had substantive similarity with authoritative guidance in the European Union by the European Commission and the European Data Protection Board.[285] Passing the act would have given some (albeit minimal) notice and choice guarantees to ensure a consent baseline, provided a clearer bar for de-identification, and discussed error rates as an issue, even without addressing distributional concerns. It would have been, in other words, a productive proportionality exercise from Congress.

The FTC FIPPs and the principle of proportionality relate to the proposals throughout this Article on how to minimize containment apps' unintended consequences. The first two principles, awareness and consent, bring into the analysis the considerations set out in Part III about how containment apps can strengthen effective notice, effective choice, and robust de-identification while remaining functional. The third and fourth principles, participation and security, provide a framework to apply the considerations set out in Part IV on how to bolster data integrity by thinking differently about different types of errors and their distribution, and how to work towards a wider participation of different social groups into the containment strategy.

If proportionality is the aim, containment apps should contain transparent design to increase user understanding and de-identify data with awareness that doing so is not a failproof privacy guarantee. In terms of the taxonomy introduced, they should minimize data retention by working on a decentralized

---

[280] *See id*. at §§ 2(6)-(7).
[281] *Id*. at § 2(9).
[282] *Id*. at §§ 3(a)-(c).
[283] *Id*. at § 3(f).
[284] Jennifer Granick, *Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?*, ACLU (Apr. 16, 2020), https://perma.cc/BWF6-BYHT (suggesting consent provisions, data minimization, restricted use, and transparency).
[285] *See* Guidance on Apps Supporting the Fight Against COVID 19 Pandemic in Relation to Data Protection, 2020 O.J. (C 124); EUR. DATA PROT. BD., *supra* note 30. (including provisions on consent, purpose limitation, data minimization, transparency, and accountability).

system. They should only collect the data they need to function, avoiding asking for information such as zip codes or ID numbers. They should have clear data retention periods: sunset clauses that include both the app and the data it collected. Contact tracing apps should operate based on Bluetooth (proximity) data rather than GPS (location) data and immunity passports should avoid continuous tracking.

These principles should be applied not only to the design but also the rollout of immunity passports. Applying them, however, does not guarantee a uniform conclusion. For some, immunity passports with regards to the people who hold them, would involve *fewer* restrictions.[286] The principle of least restrictive intervention would lead to having at least some people that are able to move freely, even if everyone would not have that opportunity. For them, immunity passports would do well in a balancing exercise. Contact tracing apps are *more useful* when there are fewer restrictions, but immunity passports *enable* fewer restrictions at least for some, and this difference is relevant for restrictions' proportionality.

For Daniel Weinstock and Vardit Ravitsky, on the other hand, immunity passports would fail the test of the least restrictive intervention with regards to equality.[287] Similarly, it has been argued that, depending on vaccine distribution, if civil liberties restrictions are made dependent on immunity passports, states could face constitutional challenges based on Equal Protection.[288] The Equal Protection Clause protects from prohibited classifications and not from disparate impact.[289] But any foreseeable rationale to roll out vaccines would be facially

---

[286] de Miguel Berain & Rueda, *supra* note 232, at 660-661 ("if a person has been tested positive for and recovered from COVID-19, becoming immune to it, she cannot be considered a hazard to public health and, therefore, the curtailment of her fundamental rights (e.g., the right to freedom of movement) is not legitimate."); Govind Persad & Ezekiel Emanuel, *The Ethics of COVID-19 Immunity-Based Licenses ('Immunity Passports')*, 323 JAMA 2241, 2241–42 (2020) (arguing that immunity passports would improve some people's situations and policy should not level down).

[287] Weinstock & Ravitsky, *supra* note 233, at 283–85 (adding that "there should be a presumption in favour of equality-promoting or at the very least inequality-minimizing measures"). *See also* Daniel Weinstock, *A Harm Reduction Approach to Physical Distancing*, *in* THE ETHICS OF PANDEMICS (Meredith Schwartz, ed., 2020) (discussing equality-favoring measures to reduce the spread of the virus); Floris Tomasini, *Solidarity in the Time of COVID-19?*, 30 CAMBRIDGE Q. HEALTHCARE ETHICS 234 (2020) (arguing that the underlying inequalities produced by COVID-19 lead to an element of solidarity that must be taken into account).

[288] David Studdert & Mark A. Hall, *Disease Control, Civil Liberties, and Mass Testing—Calibrating Restrictions During the COVID-19 Pandemic*, 383 NEW ENG. J. MED. 102, 102–104 (2020).

[289] Reva B. Siegel, *Equality Talk: Antisubordination and Anticlassification Values in Constitutional Struggles over Brown*, 117 HARV. L. REV. 1470, 1474–75 (2004); Jack M. Balkin & Reva B. Siegel,

neutral even if it has indirect pervasive effects on marginalized communities or along the lines of race, religion, or sexual orientation.[290] The analysis should be based on the correct tradeoff. Classifications based on health status would pass rational basis review, as the government has a legitimate interest not only to contain the pandemic but also to re-open the economy safely—and they may also pass strict scrutiny, as they could be considered a compelling state interest.[291] Thus, these constitutional challenges would be almost impossible to carry out successfully. Even if immunity passports pass an Equality Clause rational basis review, however, they could be considered unwarranted in a policy-oriented proportionality exercise based on that same principle of equality.

To evaluate the surveillance tradeoff in a balancing analysis, what may be most important to identify of a containment app is the baseline. Isolation is uncontroversial from a constitutional perspective.[292] It fits squarely within states' police power. Justice Harlan put it clearly in the landmark vaccination case *Jacobson v Massachusetts*, where he stated that the Supreme Court "distinctly recognized the authority of a state to enact quarantine laws."[293] Similarly, federal district courts have upheld COVID-19 quarantines for visitors and locals returning from travel when challenged.[294] Any data-driven containment measure must be evaluated against this baseline of constitutionally appropriate, isolation-based, containment measures, not to the baseline of normalcy.

American Civil Rights Tradition: Anticlassification or Antisubordination?, 58 U. MIAMI L. REV. 9, 12–14 (2003).

[290] Persad & Emanuel, *supra* note 286, at 2241–42 (comparing the restriction with age restrictions for driver's licenses). *But see* Weinstock & Ravitsky, *supra* note 233, at 285 (arguing that one can "propose that discriminating between immune and non-immune persons is analogous to the constitutionally prohibited grounds of disability").

[291] *See* Abiri & Guidi, *supra* note 262, at 18-19 (suggesting rational basis review is the appropriate test). *See, e.g.*, Roman Catholic Diocese of Brooklyn v. Cuomo, 141 S. Ct. 63 (Kavanaugh, J., concurring) ("[J]udicial deference in an emergency or a crisis does not mean wholesale judicial abdication, especially when important questions of religious discrimination, racial discrimination, free speech, or the like are raised.")

[292] From an international human rights perspective, privacy and freedom of movement are qualified rights, meaning that governments can interfere with them in cases of emergency, conditionally to a proportionality assessment—as opposed to non-derogable rights, which cannot be interfered with. Maria Pia Sacco et al., *Digital Contact Tracing for the COVID-19 Epidemic: A Business and Human Rights Perspective*, INT'L BAR ASS'N 1, 3 (2020); *see also* Eugenia Tognotti, *Lessons from the History of Quarantine, from Plague to Influenza*, 19 EMERGING INFECTIOUS DISEASES 254 (2013) (explaining that quarantine has been routinely used by law since the black death in the 14th Century).

[293] Jacobson v. Commonwealth of Massachusetts, 197 U.S. 11 (1905).

[294] *See, e.g.*, Bayley's Campground Inc. v. Mills, 463 F. Supp. 3d 22 (D. Me. 2020) (ruling that the measure was subject to strict scrutiny, rather than Jacobson's reasonableness rule, but the state had a compelling interest); Carmichael v. Ige, 470 F. Supp. 3d 1133 (D. Haw. 2020).

An appropriate balancing exercise that applies proportionality (and, by doing so, considers the principle of least restrictive intervention) will not categorically reject data-driven technology to aid in containment. Rather, it will examine how containment apps can assist healthcare workers in containing the pandemic while minimizing the harms that the ensuing surveillance produces. Conditional on rolling out an immunity passport, for example, it should be based on vaccine data, implemented only when vaccines are widely distributed, track location only at the moment it is scanned, and provide a paper option.

VI. CONCLUSION

Containment apps present important benefits for curbing the pandemic's spread. But they also introduce surveillance risks that we must consider—both at a policy level and at an individual level. The responsible response is to identify and mitigate them. The objective of this Article has been to explain how we do so and how we can arrive at a proportional conclusion.

This Article explores four interrelated risks that immunity passports and contact tracing apps create due to their type of surveillance and its distribution. Because of their commonalities, the Article calls these apps "containment apps." It discusses how different versions of containment apps create or avoid each of these risks, providing a roadmap for policymakers to choose among versions of these apps and mitigate their unintended consequences.

Legislators and judges should be attentive to and take measures to curb these four risks, both at a federal and at a state level. Although most concrete recommendations will be contextual, containment apps should focus on transparency towards users and should de-identify data while being aware that doing so is not a failproof privacy guarantee. They should work on a decentralized system. They should use the least invasive data they can (e.g., for contact tracing apps, proximity over location). And they should have clear sunset clauses for the app and collected data.

But consequences extend beyond policy. Individuals can also keep these risks in mind when deciding how to use a containment app. They can do so by, for example, selectively turning Bluetooth or GPS off to avoid disclosing information that they would rather not share, by making sure that they understand the working and consequences of an app before weighing the costs and benefits of

using it, by placing the right level of trust in apps' output, and by being judicious about drawing inferences about others.