# **Introduction: The Real Test Wasn’t the Virus**

*An empty avenue in Manhattan during the 2020 lockdown. Nearly half of humanity was under stay-at-home orders in April 2020​*

[*euronews.com*](https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou#:~:text=More%20than%203,19%20virus)

*—a collective act of social compliance unprecedented in scale.*

In the spring of 2020, bustling cities fell silent. Streets that never slept were suddenly empty, save for patrolling police and the occasional delivery van. This global pause was not just a public health response; it was a worldwide **social experiment in compliance**. When the World Health Organization declared COVID-19 a pandemic on March 11, 2020, governments in at least 90 countries swiftly imposed lockdowns that eventually confined over 3.9 billion people—**half of the world’s population—to their homes**​

[euronews.com](https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou#:~:text=More%20than%203,19%20virus)

. The *real* test posed by COVID-19 was not only medical. It was a test of how far societies would go in *obeying authorities*, suspending civil liberties, and reordering daily life under the banner of safety. While the public fixated on case counts and mask mandates, a deeper structural drama was unfolding: **power was consolidating, surveillance was expanding, and the scaffolding of future AI-driven governance was being erected in real time**.

As a researcher observing these events in 2020 and 2021, I often felt that **the virus was only the catalyst** or pretext; the more profound narrative was about control. Around the world, leaders invoked wartime language—“battle,” “fight,” “war on the virus”—and citizens dutifully lined up, figuratively and literally, to do what they were told. Entire economies ground to a halt on government orders. Democracies known for fierce independence accepted curfews and travel bans with minimal resistance. Fear of the invisible pathogen made *compliance* seem not only rational but virtuous. Yet, in the shadows of this public acquiescence, new precedents were set for how technology and executive power could be used in crises. **Emergency decrees** were issued overnight, smartphone apps began **tracking our contacts**, and algorithms started deciding who could go where. Each development was ostensibly temporary, done in the name of public health. But as this book will argue, **these measures formed a prototype of governance that could long outlast the pandemic**.

We stand at an inflection point. The pandemic **tested the limits of social control** in liberal democracies and authoritarian states alike. It taught governments that entire populations could be directed—via fear, law, and technology—toward collective behavior change virtually instantaneously. It also taught the public what it feels like to live under intensive surveillance and regulation of everyday activities. In 2020, even many who normally champion civil liberties found themselves supporting strict interventions “for the greater good.” But by 2021, cracks in the consensus were visible: protests flared from Michigan to Madrid, and courts in some countries questioned the proportionality of the restrictions. These tensions hint at the core theme of this book: **the balance between public safety and individual freedom**, and how COVID-19 accelerated a future where artificial intelligence (AI) may tip that balance decisively toward centralized control.

This first half of *The Compliance Experiment* examines the pandemic through a unique lens. Chapter 1 (this introduction) frames the pandemic response as a grand stress test of governance structures. Chapter 2 explores how governments activated **emergency powers** and the psychological levers of obedience, effectively reshaping norms of governance overnight. Chapter 3 delves into the normalization of **digital surveillance**, from contact tracing apps to biometric “health passports,” highlighting how quickly societies accepted invasive technologies. Chapter 4 pulls back the curtain on the rise of **algorithmic enforcement**—the subtle but powerful role of AI systems that enforced rules and managed information flows during the crisis. Throughout, we stay grounded in the data and events available up through 2021, drawing on reports from the World Health Organization, the U.S. CDC, *MIT Technology Review*, *The Lancet*, and other contemporaneous sources. Crucially, each chapter will end with speculative predictions framed as foresight from a 2021 vantage point—guesses, not certainties, about how these trends might evolve.

I write in a tone of *urgent analysis*, as someone who in 2020–2021 tried to see beyond the immediate crisis. While news headlines blared about ventilator shortages or school closures, I found myself tracking a parallel narrative: **How might the tools and precedents of the COVID response shape the world to come?** The chapters ahead combine personal insight with political analysis and technological foresight. My aim is to document not only what happened, but what those events *signified* for the future of governance. In doing so, I hope to show that when humanity confronts a grave threat like a pandemic, the measures we adopt can fundamentally alter our social contract. COVID-19 will eventually subside; the enhanced powers of governments and the embedded presence of AI in managing society may not.

In the end, **the real test wasn’t the virus**. The virus was a hazard to be managed. The *real* test was whether our civic institutions, our laws, and our values could withstand the temptation of authoritarian efficiency. It was a test of how readily free societies would accept controls on movement, speech, and privacy—and how those controls, once normalized, could pave the way for a new era of governance by algorithm. The following chapters chronicle that test, drawing lessons about what we got right, what we sacrificed, and what we must be vigilant about as we build a post-pandemic world.

# **2. Emergency Powers and the Psychology of Obedience**

*Police checkpoint on a highway in the Philippines during a COVID-19 lockdown (2021). Governments worldwide invoked extraordinary powers and enforcement measures in the name of public health​*

[*carnegieendowment.org*](https://carnegieendowment.org/posts/2020/04/how-will-the-coronavirus-reshape-democracy-and-governance-globally?lang=en#:~:text=Already%2C%20some%20governments%20have%20used,the%20tip%20of%20the%20iceberg)

*.*

In the early months of the pandemic, **political authority expanded at a breathtaking pace**. Leaders from across the political spectrum—democratic and authoritarian alike—declared states of emergency that granted them wide latitude to act unilaterally. By April 2020, more than 90 countries had imposed nationwide lockdowns, and many activated emergency legal frameworks to do so​

[euronews.com](https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou#:~:text=More%20than%203,19%20virus)

. In some cases, this meant presidents or prime ministers ruling by decree, bypassing legislatures and normal checks and balances. In other cases, local authorities gained broad powers to enforce curfews, business closures, and bans on gatherings. *Freedom House* reported that since the outbreak began, the condition of democracy and human rights deteriorated in 80 countries, with governments “engaging in abuses of power, silencing critics, and weakening or shuttering institutions” under the guise of virus response​

[freedomhouse.org](https://freedomhouse.org/report/special-report/2020/democracy-under-lockdown#:~:text=The%20COVID,and%20weakening%20or%20shuttering%20important)

. As one analysis by the Carnegie Endowment noted in April 2020, *“Already, some governments have used the pandemic to expand executive power and restrict individual rights”*​

[carnegieendowment.org](https://carnegieendowment.org/posts/2020/04/how-will-the-coronavirus-reshape-democracy-and-governance-globally?lang=en#:~:text=Already%2C%20some%20governments%20have%20used,the%20tip%20of%20the%20iceberg)

. What would have seemed unthinkable in January 2020—millions of people under house arrest, armies deployed to city streets, protest effectively outlawed—became a lived reality by that spring.

To be fair, **some limitations on liberty are expected in any major crisis**. Public health laws in many countries allow for quarantines and curfews during outbreaks. But COVID-19 triggered emergency provisions on an unparalleled global scale. The United States, for instance, invoked the Stafford Act and the National Emergencies Act, giving the President access to special powers and funding. **Across Europe, leaders invoked wartime rhetoric**; France declared *“nous sommes en guerre”* (“we are at war”) and empowered police to issue fines for anyone outside without official justification. In Hungary, the parliament granted Prime Minister Viktor Orbán the right to rule by decree indefinitely (a move widely criticized as opportunistic authoritarianism). From the Philippines to South Africa, curfews were enforced by armed patrols, and violators faced arrests or steep penalties. According to one study, by mid-2020 **over 100 countries** had instituted some form of emergency rule or significantly expanded executive powers to deal with COVID-19. **The pandemic, in effect, suspended normal politics.** Many elections were postponed (or hastily adjusted to mail-in voting). Courts slowed or halted operations. Legislatures often deferred to executives and health technocrats.

**The psychology of public obedience** during this period is as important as the legal mechanisms. Most citizens complied with these draconian measures—not at gunpoint, but willingly, even fervently. Panic and uncertainty created a psychological state in which people *wanted* strong leadership and clear directives. In those terrifying early weeks, many of us checked our phones daily for government text alerts or press conferences, seeking guidance and reassurance. Behavioral scientists observed that a certain level of fear can be functional: feeling personally at risk of infection was linked with greater willingness to practice social distancing and hygiene measures. In fact, one study in 2020 found that individuals with higher anxiety and fear about COVID-19 were **more accepting of government-mandated personal restrictions**. In other words, fear—often seen as a negative emotion—had a pro-social effect by motivating compliance with rules to reduce risk. Governments, perhaps intuitively, leveraged this. Public service announcements were often designed to heighten concern: showing footage of overflowing ICUs, or using slogans like “Stay home, save lives.” In the UK, a memo to the Scientific Advisory Group for Emergencies (SAGE) infamously noted that the public might need to be “frightened” into compliance, as reported by British media in 2020. Likewise, Italy’s early COVID ads featured haunting images of intubated patients to drive the severity home. **Fear, trust, and authority** worked in tandem. People trusted that these extreme rules were necessary (trust in scientists and health officials was at a record high in many places during 2020), and fear of the virus made the prospect of disobedience seem not just illegal but morally wrong.

Historical precedents can help us understand this dynamic. Social psychologists often point to Stanley Milgram’s 1960s obedience experiments, where ordinary people administered what they thought were dangerous electric shocks to others when instructed by an authority figure. The lesson: under certain conditions, **people obey authority even against their own usual moral code**. The pandemic created a “Milgram-like” environment on a mass scale. The authority figures were not lab-coat scientists but government officials and health experts. The instructions—*stay at home, do not visit even your family, close your business, accept monitoring*—would normally be blatant violations of personal freedom. Yet billions complied. Notably, **this obedience was maintained not just by force of law, but by social pressure**. Neighbors shamed neighbors who broke lockdown. On social media, viral videos would denounce an unmasked shopper or a clandestine party. In many countries, hotlines were set up for citizens to report quarantine violators. This atmosphere created what one might call *compliance culture*: a temporary norm where following the rules to the letter was equated with being a good citizen, and criticizing the rules was seen by some as antisocial or dangerous.

Of course, the story of compliance was not uniform. As weeks turned to months, **fatigue and resistance emerged**. Protests erupted: in Michigan, demonstrators occupied the state capitol in April 2020 to oppose extended lockdown orders; in Germany, the “Querdenker” (lateral thinkers) movement drew diverse crowds skeptical of COVID measures. By late 2020 and into 2021, more people began to ask whether the cure was worse than the disease—pointing to rising unemployment, mental health crises, and lost schooling. Still, it is telling that these protests were relatively limited in size compared to the overall population under restrictions. The majority remained compliant, or at least passive. In many places, courts upheld even very restrictive policies as constitutional given the emergency. Polls showed significant public support for strong measures, especially in the early phase. For example, a survey in April 2020 found majorities in multiple countries favored strict lockdowns and would sacrifice some freedoms to stop the virus. Functional fear played a role, but so did **trust in government**. In societies where people trusted that authorities were acting based on science (like in New Zealand or Finland), compliance levels were extremely high. By contrast, where trust was low or leaders sent mixed signals (as in Brazil or the U.S. under the Trump administration), compliance was more uneven and often split along partisan lines.

The use of **police and military force** to back up emergency orders was another hallmark of the pandemic response. Images from 2020 and 2021 show a startling militarization of public health enforcement: National Guard troops distributing food and manning testing centers in American cities; soldiers on the streets of Paris checking paperwork; police in India using cane sticks to disperse loiterers; and in Manila, officers at checkpoints aiming temperature guns at drivers’ heads. While often these forces were deployed for logistical help or visual deterrence rather than direct coercion, their presence sent a clear message: *the state is serious, comply or face consequences*. In some countries, abuses were reported. Human Rights Watch documented cases in places like Kenya and Nigeria where enforcement of curfews led to brutality and even deaths. Still, on the whole, **overt violence was rare** given the scale—again underscoring that *voluntary compliance* and social coercion did most of the work.

It’s important to note that emergency powers, once invoked, can develop a **momentum of their own**. Laws passed in haste tend to linger. For example, the Patriot Act in the United States, rushed through after 9/11, persisted for years with only minor changes. Similarly, many COVID emergency measures were repeatedly extended. By late 2021, some countries were still formally under states of emergency or had integrated certain mandates into ordinary law. Scholars warned early on that **“the laws and norms being put in place now will be difficult to reverse”**​

[freedomhouse.org](https://freedomhouse.org/report/special-report/2020/democracy-under-lockdown#:~:text=likely%20to%20continue%20after%20the,the%20next%20three%20to%20five)

. This proved prescient. In Hungary, the decree powers granted to Orbán were scaled back after international outcry, yet the episode left a lasting impact on Hungary’s democratic institutions. In Israel, emergency cellphone surveillance by the internal security service, launched to do contact tracing (without public debate initially), was halted by the Supreme Court after a few months, but only after data had already been collected on hundreds of thousands of people. The Israeli government kept trying to reauthorize it, citing waves of new infections. A pattern emerged globally: **temporary measures tended to become semi-permanent** or were repeatedly rejustified as new “waves” of the virus hit.

From a governance perspective, COVID-19 demonstrated both the **power and peril of emergency rule**. On one hand, decisive actions undoubtedly saved lives. Countries that locked down early and hard (like China with Wuhan, or New Zealand with its elimination strategy) did manage to control the virus more successfully in 2020. On the other hand, the ease with which emergency powers slipped into place and the breadth of behaviors regulated were astonishing. Free nations found themselves flirting with authoritarian tools: **drones shouting orders from above, phone apps tracking movements, government units monitoring online speech**. The social contract shifted: citizens were expected to surrender an expansive range of freedoms in exchange for protection from a biological threat. How willingly we did so raised eyebrows among civil libertarians. Was this prudent, temporary collective discipline? Or a slide toward a more managed society that would normalize top-down control?

*2021 Foresight:* As the crisis atmosphere recedes, the critical question is what becomes of these **expanded powers and compliance norms**. In 2021, one can already predict the tug-of-war that will shape the post-pandemic order. On one side, governments may be reluctant to fully relinquish convenient powers. We may see **“emergency” measures quietly codified into ordinary law**, justified by the need for readiness in future pandemics or even for other crises like climate change or terrorism. For example, a country might keep its travel registration system in place, turning it into a permanent visa or immigration control tool. Or surveillance powers used for quarantine tracking might be retained for general security monitoring. On the other side, publics might gradually lose their singular focus on health safety and rediscover their appetite for liberty, leading to backlash against overreach. We might see courts striking down lingering restrictions, or new political movements centered on restoring pre-2020 norms. A key predictor will be **memory and fear**: if COVID’s devastation remains vivid and other threats (like virus variants) keep health fears high, populations may continue to tolerate more control. If memory fades and normal life feels secure, intolerance for emergency rules will grow.

Another foreseeable development is the **institutionalization of “emergency expertise.”** Governments now have playbooks for lockdowns and social control that simply did not exist before. Specialized units or advisors (often including behavioral psychologists) have been integrated into government responses. Looking ahead, one can imagine these units being reactivated for any number of problems. For instance, consider a severe air pollution event or an extreme heatwave: a government might dust off the lockdown concept for environmental reasons—urging or even ordering people to stay indoors for their safety. Would citizens comply as readily as they did for COVID? Possibly, if the COVID precedent has normalized the idea that in an emergency, rights can be suspended for the common good. The risk, of course, is *mission creep*. What truly counts as an emergency? The line could blur, especially if technology makes it easier to impose and enforce restrictions without heavy economic cost. By 2021, we already see discussions about using smartphone alerts and curfews in response to natural disasters or violent incidents.

In summary, the pandemic’s legacy may include a populace more conditioned to accept rapid behavior mandates, and governments more confident in their ability to orchestrate compliance on a massive scale. The “limits of control” were stretched in 2020-21, and notably, they did not break. This success (from a control standpoint) will certainly inform governance in the future. The challenge for societies will be establishing new **safeguards**: sunset clauses, oversight committees, and clear criteria for any future emergency measures, to prevent abuse. As an author writing in 2021, I am struck by a paradox: **we passed the compliance test with flying colors**, but that very success raises alarms. In the chapters that follow, we will see how technology, in particular, made such compliance feasible and how it might be wielded in the future. Before that, however, it’s crucial to understand how deeply surveillance became normalized during the pandemic—ostensibly to ensure our obedience and safety. That is the focus of the next chapter.

# **3. Surveillance Normalized: Digital Contact Tracing and Biometric Passes**

The year 2020 will be remembered as the moment when **mass surveillance became a routine public health tool**. Faced with an invisible virus, governments and corporations turned to the *next best thing to watch it*: watch the people. Almost overnight, measures that would have caused public outrage under normal circumstances—tracking individuals’ movements via their phones, requiring digital certificates to travel, thermal cameras scanning crowds for fevers—became not only acceptable but expected. The pandemic **normalized a new level of intrusion** into personal data and bodily privacy. And it did so with surprisingly little debate at the time, as fear of disease trumped concerns about surveillance. In this chapter, we examine two of the most striking examples: digital contact tracing apps and the rise of biometric “health passes.” Both started as health responses to COVID-19, and both now seem poised to become prototypes for future high-tech governance.

## **The Global Contact Tracing Experiment**

In the early days of COVID-19, one of the biggest challenges for public health was **tracing who had been exposed** to the virus. Traditional contact tracing is labor-intensive: armies of phone callers asking infected people, “Where were you? Who did you meet?” Given the virus’s rapid spread, manual tracing couldn’t keep up. Enter **digital contact tracing apps** – a concept both simple in pitch and vast in implication. The idea: put an app on everyone’s smartphone that uses Bluetooth or GPS to log when you come near others; if someone later tests positive, the system can automatically alert everyone who crossed their path. By April 2020, this idea gained serious momentum worldwide. Tech giants Google and Apple, in a rare collaboration, developed an exposure-notification framework and rolled it out to billions of devices by May 2020. Governments from Singapore to Germany launched official apps using this Bluetooth model, emphasizing privacy (data anonymized, stored mostly on device) and voluntary use.

On paper, it sounded like a pandemic game-changer—a way to **augment human tracers with digital speed and scale**. In practice, however, the uptake and effectiveness of these apps were mixed at best. Singapore’s **TraceTogether** app was among the first, launched in March 2020, but by that summer it had stagnated at around 20-25% adoption due to privacy worries and technical hiccups​

[technologyreview.com](https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/#:~:text=Can%20these%20apps%20help%3F%20Early,In%20California%E2%80%94the%20most%20populous)

. (It also later came out that Singapore police could access the data for criminal investigations, sparking public backlash.) In Europe, countries like Iceland saw high adoption (around 40% of the population) but admitted the app had not been a “silver bullet.” Germany’s Corona-Warn-App eventually achieved over 25 million downloads, but its impact was hard to quantify. In the United States, the approach was decentralized—each state could launch its own app (often based on the Google/Apple template). By December 2020, 19 U.S. states plus D.C. had done so, theoretically covering nearly half of Americans. Yet even where available, **actual usage remained low**. Surveys indicated that many Americans either didn’t know about the apps or didn’t trust them. The *MIT Technology Review* ran a “Covid Tracing Tracker” which by late 2020 observed that lack of a national app and patchwork implementation hindered success​

[technologyreview.com](https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/#:~:text=Can%20these%20apps%20help%3F%20Early,In%20California%E2%80%94the%20most%20populous)

.

Despite these hurdles, one cannot overlook what happened culturally: **the public conversation shifted to *how* to do surveillance, not *whether***. At the start of 2020, the notion of government tracking your phone continuously would have raised howls about Big Brother. By mid-2020, that debate had been reframed. In many countries, it became patriotic to install the app—“Do your part to stop the spread.” Privacy advocates did raise concerns: for instance, in April 2020 over 300 academics signed an open letter urging that contact tracing apps preserve privacy and avoid a slippery slope to mass surveillance. This prompted some governments to adopt decentralized designs (as opposed to logging data on a central server). *The Lancet Digital Health* noted that **dozens of countries were exploring phone-based tracing despite privacy concerns**. The urgency of the pandemic provided political cover. As one French official bluntly said, “Desperate times call for desperate measures—if it saves lives, people will accept it.” Indeed, polls in the UK and elsewhere showed majority support for apps if they were clearly for health purposes.

Ironically, the **technological limitations** of these apps sometimes protected privacy by default. GPS-based tracing was often too imprecise or battery-draining, so many apps used Bluetooth signals. Bluetooth doesn’t record location, only proximity to other phones, and Google/Apple built in random rotating IDs to avoid personal identification. Still, what these apps collected was unprecedented: a continuous log of **every close encounter between individuals** who have the app. That’s a lot of intimate social data. The typical safeguards were that data would only be uploaded if a person tested positive and agreed to trigger alerts, and that alerts would be anonymous (“You were near someone who has COVID” without saying who). But even anonymized, such data at population scale can reveal patterns. Researchers warned that if not carefully handled, contact logs could potentially be re-identified by malicious actors, or later repurposed by governments. For example, in some places there were proposals to use contact-tracing infrastructure to monitor quarantine compliance (essentially flag if someone supposed to stay home is detected mingling via the app).

One also cannot ignore the **authoritarian approach to contact tracing** that emerged parallel to the smartphone apps. Not every country waited for citizens to opt in. China, for instance, went a different route with its **Health Code system** (more on that in the next section) – effectively using QR codes and mandatory phone check-ins at public venues to trace contacts and enforce quarantine. Israel invoked its internal security service to do cell phone location tracking of infected persons (an effort later curbed by court order). South Korea combined credit card records, cell tower data, and CCTV footage to do extraordinarily detailed contact tracing; then it publicly posted details of patients’ movements (anonymized, but often enough for the savvy public to guess identities). Such methods were intrusive, but South Korea’s success in containing COVID-19 in early 2020 was often contrasted with the struggles of Western countries. The implication: *surveillance saved lives*. As *The New York Times* reported in March 2020, Asian democracies like South Korea and Taiwan were deploying high-tech tracing that ran up against Western privacy norms, but with striking results in controlling the virus.

By 2021, **digital contact tracing had largely proven underwhelming in epidemiological impact**, according to assessments in *MIT Technology Review* and *Nature*. A review in *The Lancet* found that while technically the apps could alert people faster than human tracers, their effectiveness was “highly dependent” on widespread uptake and integration into public health workflows. Many countries quietly deprioritized their apps in favor of old-fashioned methods once it became clear the hoped-for adoption (often 60%+ of population) wasn’t reached. However, the experiment was hugely significant in another way: it accustomed policymakers and portions of the public to the idea of **real-time data collection on citizen interactions**. It built an *infrastructure* and knowledge base that could be repurposed. The Google-Apple API for exposure notifications still sits on hundreds of millions of phones, dormant but ready. Should another disease outbreak occur, the switch can be flipped again. And beyond health, one can imagine variants of this idea: consider disaster response (logging people in an earthquake zone to aid rescue), or even security (anonymously logging proximity to known crime suspects—which starts sounding like a policing tool). The pandemic essentially beta-tested this form of surveillance at scale.

## **Passes, Permits, and Biometric IDs**

Even as contact apps were being rolled out, another digital tool of control was stirring intense discussion by late 2020: **“immunity passports”** or health certificates for COVID. The concept initially referred to a document proving one had recovered from COVID-19 and had antibodies, theoretically granting some immunity. Health authorities like the WHO were quick to oppose this early on, warning in April 2020 that there was *“no evidence that people who have recovered… are protected from a second infection,”* and that such passports could be inaccurate and discriminatory. That quelled the idea of antibody-based passes. But soon, with vaccines on the horizon, the concept morphed into **vaccination certificates**. By the start of 2021, the conversation wasn’t hypothetical anymore—countries were actively implementing systems to distinguish between those “safe” (vaccinated or tested) and those not.

Israel moved first, launching its **“Green Pass”** system in February 2021. Israelis who were fully vaccinated or recently recovered from COVID could download a Green Pass (a QR code) to show at gyms, theaters, hotels, and other venues. This effectively opened parts of society to the immunized while restricting the unvaccinated. Denmark had a similar idea with its “Coronapas,” and plans for an EU-wide certificate were underway. In fact, the **EU Digital COVID Certificate** was piloted in spring 2021 and formally launched in July 2021, allowing EU citizens to travel freely within the bloc if they could show proof of vaccination, recent negative test, or recovery. Suddenly, **showing your health status became a prerequisite for movement**. This was a radical shift. In modern times, we haven’t had to show medical documents to get on a bus or enter a shopping mall. Now it was becoming normal to have to flash a QR code to dine at a restaurant (as was the case in France by summer 2021).

*A traveler displays an EU Digital COVID Certificate on a smartphone at an airport in 2021. Health passes like this, enabled by QR codes and often linked to biometric IDs, became gateways to travel and public life during the pandemic.*

The infrastructure behind these passes often blended **biometric identification with health data**. For example, the EU certificate isn’t biometric itself (it’s just a QR code on paper or phone), but it connects to personal identity verified in a database. In China, the Health Code apps (run on Alipay and WeChat platforms) not only gave individuals a color code (green, yellow, red) based on their health risk, but were integrated with one’s national ID number and even facial recognition systems at some checkpoints. People had to scan QR codes at every building entrance, which logged their movements centrally. The system would churn out a color: *green, you may pass; yellow or red, you are barred and may be sent to quarantine*. Importantly, in China **the criteria for these codes were algorithmic and opaque**—citizens often didn’t know why their code turned yellow or red. All they knew was that code governed their freedom to move, work, or even get groceries. It was a striking example of *algorithmic governance* (and will foreshadow our next chapter’s discussion).

Elsewhere, the approach was less draconian but still raised concerns. In the EU and U.S., discussions about vaccine passports prompted debates about **privacy, equity, and the precedent set**. Civil liberties groups like the EFF (Electronic Frontier Foundation) argued that *“paper proof of vaccination raises fewer concerns…digital passports could enable new forms of surveillance”*. The concern was that once a digital health pass system exists, it could easily be expanded: today for COVID, tomorrow for other vaccinations or even for entirely unrelated data. If a bar code on your phone is what you need to show to a bouncer to get into a club, what stops that bar code from eventually including your entire health or legal record? Government officials tried to assuage fears by emphasizing these were temporary, specific measures. The UK, for instance, publicly toyed with a COVID pass for domestic use but then shelved it (only to revisit the idea later when Delta variant hit). The **United States federally did not implement a national health pass**, leaving it to states or private sector, partly due to political resistance. Some states like New York did launch digital vaccine cards (the Excelsior Pass), while others like Florida and Texas went the opposite direction and banned any requirement for vaccine proof. This patchwork reflected how contentious the idea was.

From a technological standpoint, COVID passes were a proof of concept for a broader idea: **digital identity verification tied to personal health or risk status**. Prior to 2020, digital ID efforts (like India’s Aadhaar system or various “smart ID” cards) were usually about general identity and sometimes financial or voting systems. Now health status was part of the digital ID discussion. *The Lancet* and *Nature* ran commentaries in 2021 on the ethical design of such systems, urging privacy protections like data minimization (only disclose what’s necessary—e.g., a simple yes/no that you meet criteria, rather than detailed medical info). There were also calls for **open standards** so that one country’s certificate could be recognized elsewhere, which is exactly what the EU ended up doing at scale (over 30 countries signed on to its standard by mid-2021).

Another aspect of surveillance normalization was the proliferation of **biometric screening in public.** Airports installed fever detection cameras en masse (a modern take on the old handheld thermometer gun). Some companies marketed AI-driven thermal scanners that could detect a person with fever even in a crowd, or smart helmets that allowed police to scan passersby for high temperatures. In China and elsewhere, **facial recognition systems were adapted to work even when faces were masked**, to keep identifying people for security and quarantine enforcement. The requirement to wear masks ironically spurred advances in facial recognition algorithms (they had to learn to identify people with only the top half of the face visible). This is a subtle example of how a public health measure inadvertently boosted surveillance tech. Meanwhile, **QR codes became ubiquitous** for entry logs: in many jurisdictions, you couldn’t sit down at a cafe or enter a workplace without scanning a code at the door, which registered your presence (for contact tracing purposes). Millions of people became conditioned to this check-in ritual. What if governments decide to keep that habit for knowing crowd densities or tracking fugitives? These systems have dual uses.

One striking case of technology repurposing was in **Singapore**, which had aggressively rolled out digital contact tracing and entry QR codes. In early 2021, it came to light that police had accessed the supposedly purely health-related contact tracing data in a murder investigation, despite initial promises the data would only be for COVID containment. This caused public outcry and the government had to legislate limits on such use. The incident demonstrated the classic slippery slope: data collected for one emergency can quickly become attractive for other uses, especially law enforcement.

By mid-2021, the direction was clear: we were heading toward a world where **your phone might be as crucial as your passport** when crossing a border, and where *who you are* (identity), *where you’ve been*, and *your health status* could all be verified in a tap or scan. Proponents argued this is progress—streamlining travel, improving safety, preventing disease outbreaks by quickly identifying risky individuals. Critics saw a dystopian possibility: **a checkpoint society**, where at any given moment you might be expected to show a “green light” from some app to move freely. The metaphor of *“papers, please”* from totalitarian novels no longer felt so far-fetched, except the papers were now digital and tied into vast databases.

*2021 Foresight:* Looking forward, it’s plausible that the **health pass infrastructure** morphs into something enduring. One could foresee an international digital vaccine certificate system remaining in place for air travel, not only for COVID-19 but for any disease of concern. The International Air Transport Association (IATA) was already working on a Travel Pass app in 2021. What starts as optional could become standard: imagine booking a flight and being required to upload proof of certain vaccinations or tests into your digital profile. Over time, this could integrate with passport data, effectively linking health records with travel documents. Privacy considerations will be a battleground—some jurisdictions might insist on strict limits, others might not. The risk is that **the normalization of showing a QR code to verify your safety will extend to other domains**. Perhaps during flu season, workplaces might ask for a “flu shot badge” for entry, justified by productivity concerns. Or cities grappling with pollution might someday use a system to restrict outdoor activity on smoggy days to those who have certain health clearances.

Moreover, the combination of biometric ID and personal risk scoring may evolve. China’s colored Health Code has arguably foreshadowed a future in which each person can be algorithmically assigned a risk level (health risk now, but conceivably *security* or *credit* risk in other contexts) that determines access to public spaces. That is essentially a **social credit system with a health twist**, and it materialized practically overnight in 2020. The concern among human rights observers is that this kind of system could be made permanent under pretexts of “public safety.” The technology is relatively straightforward; it’s the public acceptance that was the real hurdle, and COVID perhaps lowered that hurdle. In free societies, we might see pushback leading to laws that ban indiscriminate personal tracking and require all such systems to be voluntary. But how voluntary is something, if opting out means you can’t participate in basic activities? For example, if a digital vaccine card remains the only convenient way to attend school or travel abroad, people are forced into the system de facto.

On a positive note, the pandemic also sparked a **countermovement for privacy-preserving tech**. The fact that Google and Apple opted for a decentralized protocol was a win for privacy; it showed that mass functionality (exposure alerts) could be achieved without creating a single surveillance database. This might influence future designs: for instance, technologists are working on ways to do verification (like vaccine proof) in a decentralized way using blockchain or cryptographic proofs, so you don’t have to expose all your data. There’s also now greater public awareness about data rights, given the many discussions about what these apps and passes do. In an optimistic scenario, the legacy of COVID surveillance could be a more informed citizenry that demands better privacy protections, and more robust laws (akin to GDPR in Europe) to constrain how data can be used.

Yet, the *compliance experiment* of 2020-21 showed that in a crisis, **surveillance can ramp up to levels previously seen only in sci-fi, and society will adapt**. We lived through an era when one’s movements, contacts, and even body temperature became potentially reportable and trackable by authorities. That genie will not fully go back into the bottle. The next chapter will delve even deeper into what was happening behind the scenes: the algorithms and AI systems quietly powering many of these surveillance and control measures. If contact tracing and passes were the visible tools, there was also an invisible infrastructure of code making decisions – an incipient form of AI-led governance. How that operated, and what it forebodes, is our next focus.

# **4. The Rise of Algorithmic Enforcement: AI Behind the Curtain**

By 2021, it had become clear that much of the heavy lifting in pandemic management was being done not by human officials directly, but by **algorithms working in the background**. From deciding what information people saw on social media to flagging who might be breaking quarantine, artificial intelligence (AI) and automated systems were quietly enforcing rules and norms. COVID-19, in a sense, accelerated the handover of certain governance tasks from people to code. In this chapter, we peel back the curtain on these systems: the algorithms that filtered misinformation online, the machine-learning models that allocated police resources and health interventions, and the nascent AI tools that monitored public behavior (like mask-wearing and social distancing) without constant human oversight. The public’s attention in 2020 was on masks and vaccines, but **future historians may note that this was the moment when algorithmic governance took a leap forward under the pressure of a global emergency**.

## **Policing the Infodemic with AI**

One of the earliest battlegrounds of the pandemic was **information**. The Director-General of WHO warned in February 2020 that alongside the epidemic, we faced an *“infodemic”* of misinformation. Almost immediately, major tech platforms began deploying AI to curb COVID-related falsehoods and dangerous content. **Facebook**, for example, ramped up its content moderation algorithms. In part this was necessity: human moderators were sent home due to lockdowns and privacy issues (they couldn’t review sensitive user data from home). So Facebook leaned heavily on automated systems to detect and remove or downrank posts about bogus cures, conspiracy theories about 5G towers spreading the virus, or false claims about vaccines. In May 2020, Facebook’s VP of Integrity published a blog noting that the company was using AI to take down COVID misinformation “at an unprecedented scale” since human review was limited. According to Facebook’s transparency reports, during the first half of 2020 they removed millions of pieces of content for COVID misinformation, many of which were identified by AI proactively before users even reported them.

**YouTube** and **Twitter** did likewise. YouTube’s CEO said their AI systems were catching 94% of the violative content in some categories. Twitter introduced automated labels that would appear on tweets containing contested COVID claims, linking to authoritative info. They also relied on machine learning to prioritize which tweets needed human review. The scale of this automated enforcement was staggering. In one quarter of 2020, YouTube’s algorithms reportedly removed over 11 million videos (not all COVID-related, but significant overlap) – far more than what humans removed. The companies admitted the AIs sometimes over-censored (taking down legitimate content by mistake) but argued the urgency of the pandemic required erring on the side of caution.

This was a watershed for **AI governance of speech**. Never before had there been such a coordinated, global effort to control what information circulated, and it was largely done through algorithms trained on what *not* to allow. To the average social media user, this might have been invisible – perhaps you just noticed fewer crazy rumors in your feed, or you saw generic warning labels on certain posts. But behind the scenes, the *“algorithmic curators”* were working overtime. And interestingly, there was broad public support for this in 2020. Fear of misinformation killing people (like someone drinking bleach because they read it was a cure) made even free-speech absolutists concede that platforms should be aggressive in moderation. Governments pressured platforms to act, but also *outsourced* a lot of the task to them. Facebook, Twitter, and Google essentially became **agents of public health policy**, using AI as their tool. This public-private tech cooperation in an emergency was unprecedented: for example, Facebook and Google also collaborated with researchers by sharing anonymized user mobility data to help predict outbreaks.

The implications for the future are mixed. On one hand, this showed that AI can be marshaled to combat dangerous disinformation, which could be a positive template for other crises (e.g., climate change misinformation). On the other, it raised concerns about **censorship and error**. AI is only as good as its training data and rules; early in the pandemic, some legitimate debate (for instance about masks effectiveness or lab-leak theories) might have been stifled because it got flagged as misinformation. Moreover, extremist groups quickly adapted with coded language to evade AI detection. The cat-and-mouse game of moderation became more sophisticated. *The Verge* pointed out that Facebook’s AI for content had a blind spot: it could detect obvious keywords but struggled with nuanced context. Still, if the pandemic was an experiment, the results showed **AI could handle the volume** of global content policing better than an army of humans (albeit imperfectly). This likely means that in the long run, the balance will tip further toward automated moderation on all platforms, with human oversight on edge cases.

## **Automated Obedience: AI in the Physical World**

Perhaps more startling was how AI moved into the **physical enforcement of pandemic rules**. Consider the measures taken to ensure people wore masks and kept their distance in public. In 2020, several companies rapidly modified their existing CCTV analytics products (initially meant for things like retail footfall counting or security) to measure mask compliance and distancing. For instance, software using computer vision could scan a store’s security camera feed and alert management if customers weren’t wearing masks or were forming a crowd. Municipal authorities in cities in France, the U.S., and India piloted such systems to monitor compliance in markets and transport hubs. These systems were essentially *“AI compliance officers”*. Instead of a human guard telling you to spread out or pull up your mask, an algorithm watched, and in some cases even issued automated warnings over speakers.

Drones provided another vector. As noted in the previous chapter, **drones with loudspeakers** were used in countries like China, Spain, and Indonesia to patrol streets and scold people for violating lockdown or not wearing masks. The decision of where the drone goes and whom it addresses can be manually directed, but increasingly, AI can be involved—for example, identifying a gathering via camera and then navigating the drone there. Some drones were outfitted with thermal cameras and reportedly even CO₂ sensors (to detect respiratory signs of illness) with AI analytics to scan crowds for potential fevers or coughing. This “pandemic drone” technology was still experimental in 2020, but it demonstrated the concept of **remote, autonomous health surveillance**. It doesn’t take much imagination to foresee future drones doing the same for other purposes—crowd control at events, finding suspects, etc.—with far less public resistance now that people have seen it in action for a health reason.

One particularly science-fiction-like deployment was in **Singapore’s use of the robot dog “Spot.”** This four-legged machine, made by Boston Dynamics, was sent to patrol a public park and play recorded messages reminding people to maintain social distancing​

[smithsonianmag.com](https://www.smithsonianmag.com/smart-news/singapore-using-robotic-dog-enforce-proper-social-distancing-during-covid-19-180974912/#:~:text=Since%20May%208%2C%20the%20automated,who%20isn%E2%80%99t%20practicing%20safe%20distancing)

​

[smithsonianmag.com](https://www.smithsonianmag.com/smart-news/singapore-using-robotic-dog-enforce-proper-social-distancing-during-covid-19-180974912/#:~:text=patrols%20and%20minimizing%20physical%20contact,%E2%80%9D)

. Equipped with cameras and AI, Spot could navigate the park and even estimate group sizes. While it was technically remote-controlled during its trial, it points to a future where robots could enforce rules autonomously in public spaces. The public reaction in Singapore was curious bemusement; many welcomed it as a clever solution. This contrasts with how such a thing might have been received pre-pandemic (imagine a robot telling you how to behave in a park—many would have found that dystopian). COVID-19 made us more welcoming of such innovations if they promised safety.

Behind these visible examples, **countless algorithms churned through data to make enforcement decisions**. Cities worldwide tapped into traffic and mobility data to decide where to set up roadblocks or how to adjust curfew hours. Some police departments reportedly used predictive models (which areas are likely to have illegal gatherings?) to guide patrols. In the UK, an AI company created a system to predict which hospital might violate ICU capacity next, so authorities could preemptively redistribute resources or perhaps enforce stricter local lockdowns. In essence, governance started to look like a **data science problem**: feed in a bunch of inputs (case numbers, mobility, compliance rates, etc.), run simulations or predictions, output a recommended policy or enforcement action.

Perhaps the most consequential algorithmic system was the **health risk scoring** mentioned earlier with China’s Health Code. Here we see an algorithm directly controlling individual freedom: the code uses data and criteria (some known, some secret) to assign you a color status. If red or yellow, you’re effectively under a travel ban and must isolate. If green, you may go about life. This is a clear-cut case of *algorithmic enforcement*: a person doesn’t decide case-by-case if you should quarantine, a system does, and it’s integrated everywhere you go via QR checkpoints. Chinese citizens on forums like Zhihu expressed astonishment, feeling “ruled by algorithms” decades sooner than they expected. Importantly, the lack of transparency meant people experienced the algorithm as capricious or overly cautious. There were anecdotes of people in perfectly fine health stranded because their app turned red due to some data glitch or because they unknowingly had contact with a case. While China is a unique environment in terms of surveillance acceptance, the *function* of the Health Code could tempt other governments in future crises: it’s efficient, scalable, and from a public health view, effective in cutting transmission. The trade-off is individual rights and due process. An algorithm might tell you “computer says you’re high risk, so you lose liberty for 14 days”. We have not had such algorithmic gatekeeping widely in democracies...yet.

Even outside of health, the pandemic’s pressures accelerated adoption of AI in governance in subtler ways. Unemployment systems in the U.S., dealing with tens of millions of claims, turned to automated fraud detection that sometimes wrongly flagged gig workers. Courts experimented with virtual proceedings and some started using AI scheduling. Schools that went online used proctoring software with AI to catch cheaters (which raised alarms as the software sometimes falsely labeled nervous eye movements as cheating). All these are part of a larger tapestry: **when humans were removed from the loop due to social distancing, algorithms filled the gap**. This sudden reliance is likely to have a lasting effect. Once institutions invest in these tools and workflows adapt, there is a tendency to keep using them even after the immediate need passes.

*2021 Foresight:* We can anticipate that the **next wave of governance innovation will heavily feature AI decision-making**, justified by the COVID lesson that “it works in a pinch.” The public might be more prepared to accept AI oversight, having seen it deployed for a “good cause.” Key areas to watch include:

* **Public Surveillance**: We may see permanent implementation of computer vision systems in cities for monitoring crowd density, mask compliance during flu seasons, or general civil obedience. The argument will be that these systems can provide early warnings for emergencies (health or security). The challenge will be preventing mission creep into total surveillance. If people get used to cameras scanning for health, they may not notice when those same cameras start scanning for, say, jaywalking or other rule-breaking, issuing automated fines.
* **AI in Law Enforcement**: COVID gave law enforcement agencies a taste of using unconventional data (like anonymized smartphone location data) to do their job. There’s a risk that normalized access to such data could continue for crime prevention. For instance, if authorities could get telco location data to ensure quarantine, they might later want it to track curfews or curtail protests. Unless laws explicitly forbid it, the technical capability is there. On the flip side, the crisis also spurred new oversight—courts might be more alert now to unchecked surveillance, given the debates we’ve seen.
* **Automated Social Controls**: The idea of an app or system automatically dictating what you can or cannot do might expand. One can imagine workplace health policies where AI systems decide if you’re fit to enter the office (an evolution of those morning symptom check apps many workplaces used). Insurance companies might give discounts if you use an app that monitors your lifestyle “for health” – a voluntary but incentivized form of surveillance. The line between voluntary and required may blur, as it did with contact tracing apps that started voluntary but in some places became effectively required for entry into public buildings.
* **AI Policy Simulations**: Governments will likely increasingly use AI modeling to make policy. Pandemic modeling software guided many decisions (when to lock down, how to allocate vaccines). The success of those models (despite some controversy) means in future economic or environmental crises, leaders might lean on AI predictions to justify interventions. That could be positive if it brings more rational decision-making, but it also raises accountability questions: if an AI model says “lockdown now” and the government does it, who is accountable if that model was flawed?

One more domain deserves mention: **international coordination via data**. During COVID, AI was used to forecast global spread and coordinate responses. This might lead to more integrated global surveillance systems, maybe under WHO, using AI to detect outbreaks or biosecurity threats in real time by scanning social media, hospital data, etc. Essentially a planetary immune system driven by AI. If done transparently and with privacy, it could be a boon to humanity. However, if done opaquely, it could concentrate enormous power over global movement and trade in the hands of a few algorithm guardians.

In concluding this chapter and looking ahead, we should acknowledge a key insight: **people complied not just because of trust in government, but often because invisible algorithms structured their choices**. Your Facebook feed was scrubbed of anti-mask rants, so you saw more posts encouraging compliance, subtly shaping norms. Your phone reminded you that you were near someone infectious, prompting you to self-isolate even if no human told you to. Your workplace’s entry scanner told you to go home because you registered a fever. Multiply these micro-enforcements across society, and you see how behavior is guided by code. By 2021, we have lived through an existence proof that **AI can help manage a society in crisis**. The next question is: will it manage society in normal times too?

As someone observing in 2021, I predict that the legacy of this period will be a double-edged sword. On one edge, we have powerful new tools to **keep people safe and coordinate action**—tools that could help with everything from climate disasters to reducing crime or traffic fatalities. On the other edge, we have a potential **architecture of control** that could be misused to curtail freedoms in ways that are hard to perceive or resist, because they come packaged as recommendations from our apps, or decisions made by “neutral” algorithms. Navigating this will be one of the great governance challenges of the coming decade. The experiment is ongoing, and we—citizens, technologists, policymakers—are all participants in figuring out the balance.

In the second half of this book (beyond these chapters), we will further explore how these trends might play out, examining scenarios and strategies for preserving human agency in an age of intelligent machines and emergency norms. But as of 2021, one thing is evident: **COVID-19 has fundamentally shifted the Overton window of what forms of control and surveillance are possible and acceptable**. We have witnessed how quickly the extraordinary can become ordinary. The task ahead is to ensure that the hard-won lessons of this crisis are used to empower communities and safeguard health *without* permanently eroding the liberties and privacy that define open societies. The compliance experiment showed us both the capabilities and the dangers of our new tools. It’s up to us, moving forward, to choose how to apply them.

Chapter 5: How Crisis-Era Compliance Mechanisms Could Be Normalized and Repurposed

The Slide from Emergency to Everyday. In early 2020, governments worldwide rushed to enforce public health measures that would have seemed unthinkable just months prior. Lockdowns confined billions to their homes, emergency decrees restricted travel, and digital contact tracing apps sprang up almost overnight. These extreme compliance mechanisms were justified by the crisis—but history teaches that powers assumed in emergencies can long outlive their original purpose. Surveillance measures enacted to fight COVID-19 “threaten to accelerate the concerning normalization of surveillance and technological encroachments on civil liberties around the world”, as one international network of researchers warned . Already during the pandemic, health data and tools were bleeding into other uses: “some governments have allowed information gathered for public health purposes to be accessed by law enforcement or intelligence services” . What began as short-term, lifesaving interventions could quietly become permanent fixtures of governance. In this chapter, we examine how crisis-era compliance tools might be normalized and even repurposed for purposes far beyond public health.

Temporary Measures That Linger. Around the world, COVID-19 propelled authorities to expand their powers in ways not seen in generations. Stay-at-home orders and curfews, enforced by police checkpoints and fines, habituated citizens to stringent movement controls. Mobile phone apps and QR code systems, rolled out to trace infections, built an infrastructure for population tracking. In liberal democracies and authoritarian states alike, leaders promised these measures were temporary. Yet experience shows that unless checked, emergency powers often linger. In Israel, for example, the domestic security agency (Shin Bet) was authorized to use its counterterrorism phone surveillance tool to trace virus carriers—a repurposing of a secretive database called “the Tool” . Civil liberties groups sounded alarms, and by March 2021 Israel’s own Supreme Court intervened, noting it “feared the mobile phone tracing, imposed as a temporary emergency measure, was slowly becoming permanent” . The court banned the sweeping use of this surveillance, calling it a “grave infraction of civil liberties” . This episode illustrates the risk: extraordinary monitoring techniques, if not sunset, can slide into the new normal of governance until courts or public outcry force a rollback.

Sunset Clauses vs. the ‘New Normal’. To prevent normalization, legal experts stress the importance of sunset clauses—automatic expirations for emergency surveillance. The European Union in April 2020 urged that digital contact tracing systems include built-in data deletion and end-dates . Privacy scholars similarly argued that pandemic tech should self-terminate. A Lancet Digital Health piece in mid-2020 advocated an “application self-destruction strategy” whereby “once the pandemic is over, all … personal data is deleted” from devices and servers . The authors insisted that personal data collected for COVID-19 must not outlive the crisis . These safeguards acknowledge how easily emergency powers ossify into everyday control if not actively dismantled. Indeed, without enforced sunset provisions, infrastructure built in a crisis often remains in place, ready to be reactivated or quietly repurposed. As one policy report put it: “Requiring ‘sunset clauses’ can reduce risks that crisis-era surveillance practices become normalized” . Unfortunately, not all pandemic measures came with an expiration date—leaving a gray zone in which yesterday’s exceptions can become tomorrow’s rules.

Case Study – Health Apps Turned Permanent. Nowhere is this dynamic clearer than in the realm of COVID-19 health apps and QR codes. In China, citizens widely adopted a tri-color “health code” on their smartphones in 2020, which dictated movement: green to travel, red or yellow to quarantine. Officially, these QR codes were a temporary response. Yet observers in 2021 already questioned if they would truly disappear. Early analysis indicated the health code system was being folded into everyday life even as infections waned . One legal scholar noted the “prolonged, expanded, and normalized use of tools that were originally intended for … pandemic surveillance” and their “functional transformation … to instruments of behavior modification and social governance” . In plainer terms: a phone app that began by flagging virus risk could evolve into a general-purpose social control tool—a Data Leviathan, as the scholar warned . While that particular phrasing came later, the pattern was visible by late 2020. Chinese authorities built an unprecedented data alliance between tech firms and the state during COVID-19, legitimized by a narrative of collective security over individual privacy . Absent pushback, it was easy to foresee these systems sticking around to monitor everything from travel to dissent. By institutionalizing such tools, a government gains a dial it can turn for any perceived threat, health-related or not.

Other countries likewise showed signs of mission creep in pandemic tech. Singapore’s TraceTogether app, initially voluntary, became required for entry to workplaces, malls, and schools . Residents got used to scanning a QR code everywhere they went. Late in 2020, Singapore officials admitted that data from TraceTogether, contrary to initial promises, had been accessed by police in a criminal investigation, sparking public controversy. What was pitched purely as a public health tool had already been repurposed for law enforcement—an example of how quickly the barrier between health data and police data can crumble. In Australia, too, police sought access to data from the government’s COVIDSafe app for unrelated investigations, despite assurances to the contrary (a request that was denied amid public backlash). Each instance reinforced the slippery slope: when masses of data are collected “for our safety,” other powerful interests will want to tap into it.

From Public Health to Policing. The repurposing of compliance mechanisms is not just a hypothetical danger—it happened in real time during the crisis. Law enforcement and intelligence agencies found the newly amassed pools of data hard to resist. According to one global analysis, information gathered via COVID surveillance has been shared or requisitioned for policing in multiple countries . In the United States, for example, some cities explored using aggregate mobility data (from cell phones) to monitor compliance with stay-at-home orders. Washington, D.C. accepted a free offer from a data broker for access to its “highly sensitive” device-level GPS location database, covering the entire metro area . The rationale was COVID containment, but it highlighted how private-sector surveillance capital could easily merge with state needs in an emergency. Without strong oversight, such public-private data pipelines may persist long after the pandemic, fueling routine police monitoring or commercial analytics.

The pandemic also accelerated use of counter-terrorism tools on civilian populations. Beyond Israel’s Shin Bet tracking noted earlier, consider how other national security infrastructures pivoted inward. In some European countries, intelligence services were tasked with mapping infection spread using phone metadata normally reserved for counterintelligence. These arrangements were often shrouded in secrecy. Only later did details emerge, such as how certain telecom firms directly fed anonymized (and sometimes not-so-anonymized) mobility data to governments during lockdowns. While emergency legislation often authorized these data grabs, few countries have detailed plans to dispose of the data or dismantle the analytic systems built on top of them.

Institutionalizing Bio-Surveillance. Many of the compliance measures from the COVID era could be institutionalized under the banner of preparedness. Public health authorities, emboldened by their successes (and mindful of failures), are now arguing that we must build permanent capacities to test, trace, and enforce in future outbreaks. This makes sense from a purely epidemiological standpoint—why scramble to reinvent the wheel when a new pathogen emerges? However, the institutionalization of pandemic measures raises a vital question: Will society tolerate round-the-clock surveillance “just in case”? COVID-19 gave a prototype for algorithmic control of populations in the name of safety. We saw that it is technically feasible, for instance, to track nearly everyone’s movements via phones and credit card use, to automatically deny entry to public spaces if someone’s health/vaccine status isn’t verified, and even to deploy AI cameras to catch rule-breakers (from maskless pedestrians to curfew violators). Normalizing these practices means they could be switched on not just for a once-in-a-century pandemic, but for more routine policy goals.

We are already seeing language of normalization creep into policy. The World Health Organization and World Bank in late 2020 began encouraging countries to integrate digital health credentials and contact tracing as part of “resilient recovery” strategies . The thinking is to make these systems a permanent layer of public health infrastructure. “Countries that had this infrastructure in place before the pandemic have been able to respond more quickly,” noted the World Bank, urging accelerated rollout of digital ID and data-sharing platforms as a lesson learned . In other words, build the tracking and compliance tools now so they’re ready for the next crisis. The risk is that once built, these systems won’t remain parked in the garage until the next fire—they’ll be driven out for errands, perhaps unrelated to any health emergency.

Opportunistic Repurposing by Tech and Government. The marriage of Big Tech and Big Government during the pandemic also set the stage for repurposing. In the spring of 2020, Google and Apple rolled out an Exposure Notification API that effectively put a contact-tracing capability on billions of phones. While they implemented privacy protections (a decentralized design that stored contacts only on-device), this framework marked the first time tech giants directly shaped public health policy tools at global scale. Visionary thinkers like Naomi Klein quickly pointed out that tech corporations saw COVID-19 as an opportunity to extend their reach. She described a “pandemic shock doctrine” in which Silicon Valley pushed into every aspect of civic life, creating a “Screen New Deal” of tele-everything and datafication . According to Klein, our months of isolation were treated as “a living laboratory for a permanent – and highly profitable – no-touch future” .

In this future, convenience and safety are packaged together and used to justify constant monitoring. Tech firms, often in partnership with governments, can repurpose the sensor networks and platforms originally stood up for virus control into general systems of administration and profit. For example, digital QR code passes used for vaccine verification could morph into all-purpose digital IDs that you need to show for every flight, job, or bank transaction. This isn’t speculative—it was in the contracts. In New York State, the Excelsior Pass (a COVID-19 vaccine passport app) launched in 2021. A watchdog group later uncovered that IBM’s contract for Excelsior included a planned “Phase 2” expansion: a far larger budget and the ability to include driver’s licenses and other personal records in the app . The initial public health application was just step one; the vision was clearly to repurpose the platform as a broad digital identity system. Tellingly, New York rushed to roll out the pass without robust privacy legislation in place; a bill to protect COVID data was introduced only after the app’s launch, and it “was never taken up” by the State Senate . The safeguard lagged behind the deployment of the tech, illustrating how easily urgency can bypass accountability.

Data, Once Collected, Will Find New Uses. There is a saying in surveillance policy: data collected for one purpose will inevitably find another. COVID-19 generated oceans of data—on people’s movements, contacts, health, purchases, and communications. All of it was exceptionally valuable not only to epidemiologists but also to marketers, insurers, intelligence analysts, and political strategists. Participants in one U.S. study expected as much: they believed any app tracking health data for COVID would end up “shared with unknown third parties for the financial gain of the app makers,” effectively aligning with the business model of surveillance capitalism . Indeed, tech companies did move to monetize pandemic-related data. We saw startups pivot to “COVID surveillance solutions” for workplaces, selling AI camera systems that ensure employees keep their distance and wear masks – but those same systems could easily be rebranded for general HR compliance or security after COVID. Traditional data brokers started packaging “COVID mobility” datasets for city planners and advertisers. There is a real concern that the public health emergency served as cover to vastly expand data collection in everyday life, with the public gradually habituated to it.

Another vector for repurposing is border control and travel. Immunity passports or vaccine certificates were introduced by many countries to filter incoming travelers. But once a digital health certification system is in place at borders, it could merge with existing border surveillance (like passenger name record databases or facial recognition at airports) and persist indefinitely. The International Air Transport Association (IATA) even floated making its Travel Pass app a permanent digital travel credential beyond COVID status. Similarly, the European Union’s Green Pass initially for COVID could conceivably be extended to other vaccinations or even non-health credentials in the future, effectively becoming a normalized part of freedom of movement in Europe. Each extension would represent a repurposing of a crisis tool into the fabric of daily governance.

The Psychological “Normalization” of Control. Equally important is how public attitudes adjust to new controls. During the pandemic, many citizens accepted sweeping rules that infringed on personal freedoms—because the threat felt immediate and grave. Over time, repeated compliance can breed familiarity and even expectation. For example, being asked to show a health pass to enter a restaurant, while jarring at first, quickly became routine in some cities by late 2021. Psychologically, once people have lived under a certain regime of checks and restrictions, they may come to see it as an acceptable norm, especially if framed as for the common good. This sets the stage for those mechanisms to be used in other contexts without as much resistance. If you’ve gotten used to authorities checking your phone at highway stops to verify you’re allowed to travel (as happened in some countries during strict lockdowns), you may be less shocked when, say, a similar checkpoint is later used to search for criminals or verify car insurance. Crisis compliance measures effectively train society in a new baseline of surveillance. That training doesn’t automatically vanish when the crisis does.

Crucially, the pandemic normalized behavioral tracking on a mass scale. Activities that were once private (meeting a friend, attending a religious service, going to work) were now logged in databases in the name of disease control. In South Korea, where aggressive contact tracing included accessing credit card records and CCTV footage of infected individuals’ movements, citizens were suddenly confronted with the reality of ubiquitous tracking. Although these methods were largely accepted due to the emergency, they spotlighted a surveillance capacity that can be repurposed. Without legal barriers, what stops a government from using the same infrastructure of credit card trails and CCTV to track, say, political dissidents or tax evaders? The precedent has been set that under certain conditions, comprehensive tracking of citizens is not only possible but broadly tolerated.

Repurposing Compliance Culture. Beyond technology, COVID-19 may leave a legacy in administrative culture—the idea that compliance-by-default is a legitimate expectation from the public. Governments learned during the crisis that clear, consistent messaging combined with a dose of fear can lead the majority of people to follow even very strict rules. This has undoubtedly been noted by policymakers far outside the health domain. Already, one hears argumentation like: “We successfully mobilized society to achieve X (flatten the curve); now why not mobilize similarly for Y?” (insert any major societal challenge, from climate change to counterterrorism). The temptation to re-use the compliance playbook is strong. Some commentators have even speculated about “climate lockdowns” in the future – not literal home confinements, but drastic government actions justified by a planetary emergency. Whether or not such ideas gain traction, the point is that the pandemic response created a proof of concept for rapid behavioral engineering at scale. That concept can be repackaged and redeployed.

We must also consider repurposing by autocratic regimes. For more authoritarian governments, the pandemic provided political cover to intensify surveillance and quash dissent. Countries with poor human rights records could cynically label dissidents or minority groups as public health threats, using lockdown rules or contact tracing as tools of repression. There were reports in 2020 of some regimes leveraging COVID restrictions to break up protests and harass opposition figures under the guise of enforcing virus safety. Those tactics, once honed, become part of the toolbox for maintaining control. A troubling example came from China (again): reports emerged that health code apps were manipulated to prevent would-be protesters from traveling (by turning their code from green to red arbitrarily). While this particular revelation came after 2021, it was the logical culmination of trends visible earlier. By 2021, observers already feared that “tools used to fight for public health [could] be subverted … as cover for unrelated, unnecessary data collection” , effectively turning into systems of political or social control. The groundwork for such subversion is laid when emergency measures lack strict boundaries.

Guardrails or Perpetual Emergency? The central question is whether societies will install guardrails to prevent crisis-era mechanisms from becoming permanent governance fixtures. Will we delete the data, dismantle the apps, rescind the legal authorities granted under COVID-19? Or will we slide into a state of perpetual emergency footing, where the infrastructure of compliance stands at ready for use at the slightest provocation? The Israeli Supreme Court’s insistence on halting phone surveillance before it became entrenched was one bright spot, showing that democratic institutions can yank the leash. Similarly, multiple countries, including some U.S. states and European nations, allowed their emergency orders to expire and even outlawed certain practices (for instance, some U.S. states passed laws in 2021 banning governments from issuing digital vaccine passports, specifically to prevent long-term tracking of citizens’ health status). These are attempts to put the genie back in the bottle.

Yet the broader trend seems to be a normalization, if not in law then in practice. Many contact tracing apps around the world have not been fully decommissioned – they remain downloadable, some pivoting to general public health information apps. Surveillance cameras installed to monitor mask-wearing on streets aren’t being taken down; instead, they’re simply being redirected to standard security use. Governments now have pandemic experience to point to when arguing for expanded powers: Remember how well compliance worked to save lives? Why not use similar methods to save lives from other threats (crime, drugs, etc.)? This rhetorical shift is subtle but possible, and elements of the public, having gone through the collective trauma of COVID-19, might be amenable to it if framed compellingly.

2021 Foresight: The Fate of Crisis Technologies

• Digital Infrastructure Without End: As of 2021, it is foreseeable that many nations will quietly keep their COVID-era digital infrastructure operational. By the mid-2020s, today’s vaccine certificate apps could be merged into national digital ID programs, normalized as everyday credentials for accessing buildings, transportation, or services. What was billed as a temporary health pass may evolve into a de facto internal passport system that people use (and are tracked by) each day .

• Policing and Intelligence Use-Cases: In the coming years, expect law enforcement and intelligence agencies to lobby for continued access to the data troves generated in the pandemic. If unchecked, by 2025 we might see health-related data analytics repurposed for crime prediction or protest monitoring. Data-sharing agreements between health departments and police—once an emergency exception—could become institutionalized norms, blurring the line between public health and public safety .

• Permanent “Guardian” Technologies: Governments might normalize AI surveillance systems initially deployed for COVID compliance. For example, AI cameras that counted mask compliance could remain in use to monitor other forms of rule compliance in public spaces. Drone fleets that patrolled streets during lockdowns might be kept for general crowd control or “safety monitoring.” By 2030, society could find itself surrounded by a lattice of always-on compliance tech born in 2020, unless deliberate efforts are made to disable it.

• Adaptive Public Acceptance: On the social side, people’s expectations of privacy may continue to erode. If large portions of the public come to tolerate or even expect that governments will track locations and require digital proof for various activities, we could enter a phase where opting-out is nearly impossible. A May 2020 Gallup poll already showed a majority of Americans prioritized stopping COVID-19 spread over protecting personal privacy . Projecting forward, that trade-off mentality could extend to other domains (e.g. “stop crime/terrorism even if it means less privacy”). The net effect is a populace more amenable to surveillance, having been conditioned during the pandemic to see it as normal and necessary.

• Battle Between Sunset and Entrenchment: Looking ahead, a tug-of-war is likely. Privacy advocates and some regulators will push for sunset and rollback of emergency powers—demanding, for instance, that all COVID tracking data be purged by a set date and that any reactivation of such systems require new approval. Meanwhile, security-minded officials may quietly resist or find new justifications to keep the systems running. By 2030, the outcome of this battle will determine whether “crisis tech” lives on. The optimistic scenario is that robust legal guardrails and public pressure force most of these mechanisms back into dormancy until truly needed. The pessimistic scenario is a world where the infrastructure of pandemic compliance becomes a permanent feature of governance, repurposed in ways we only begin to imagine today.

Chapter 6: The Post-Pandemic Governance Model – Algorithmic Law, AI Enforcement, Digital ID Systems

The COVID-19 crisis of 2020–2021 accelerated a radical shift in how governments govern: rules once set on paper were increasingly encoded in apps and algorithms. In the span of months, public health measures became algorithmic law – enforced automatically by software, cameras, and AI – and digital ID systems emerged as gateways to civic life. Authorities around the world openly justified expanded surveillance powers as necessary for the pandemic, deploying technologies that only a year prior might have been deemed dystopian . A new governance model was prototyped in real time, one in which compliance was not merely requested by officials but programmed into the daily routines of billions of people.

From Emergency Law to “Algorithmic Law”

In early 2020, governments enacted emergency laws to control viral spread – curfews, travel bans, quarantines, mask mandates. But crucially, enforcement of these rules quickly transcended traditional policing. It moved into the digital realm, where code is law: software and databases automatically determine who is allowed to go where, when, and with whom. Algorithmic law refers to this phenomenon of rules being encoded into algorithms and enforced by technological systems rather than solely by human officers or courts.

One striking example emerged in Israel, typically a liberal democracy. In March 2020, the Israeli government repurposed a counter-terrorism surveillance system run by the Shin Bet security agency to track citizens’ cellphones for contact tracing . Location algorithms identified people who had been near known COVID-19 cases and automatically sent them text messages ordering them to quarantine . There was no human case investigator making a polite phone call – instead, an algorithm flagged you, and the “law” (quarantine order) was delivered via SMS. The program was highly controversial, with critics saying the state was “spying on its own citizens” . By 2021 Israel’s Supreme Court intervened, ending the blanket phone tracking over concerns that such mass surveillance could become permanent . The court warned of Orwellian dangers if emergency measures were not curtailed, noting how easily temporary powers might morph into routine governance.

Israel was not alone. China, already known for extensive digital control, pushed the paradigm even further. The government built a nationwide “health code” app system that essentially wrote pandemic rules into software. Every citizen received a color-coded QR code on their phone that dictated their freedom of movement . Green meant you could pass through checkpoints and travel; orange or red automatically mandated home isolation for 7 or 14 days – enforced by the app’s integration with public venues and transport . To obtain this code, individuals had to upload personal data – national ID number, a biometric selfie, health symptoms, travel history – into the government app . Behind the scenes, AI algorithms analyzed each person’s data and interactions to calculate a risk score . In effect, a software system was given authority to dictate quarantine orders and travel permissions – a pure example of algorithmic law governing daily life.

Such systems often operated with opaque logic. Many Chinese citizens could only guess why their code turned red or stayed red longer than expected . Some suspected it was due to being from a high-risk region or a data error . Regardless, there was little room to appeal a code assignment – the algorithm’s decision had the force of law, at least until one could get re-tested or cleared through bureaucratic hoops. This lack of transparency or “avenues for redress” was a common feature across emerging algorithmic governance measures . In the urgency of the pandemic, due process often fell by the wayside. As Freedom House analysts observed in 2020, COVID-19 created an opening for the collection of intimate data without adequate oversight, and governments began using AI and big data tools to make decisions affecting individual rights – often without transparency or independent review .

Other countries also encoded pandemic rules into automated systems. Hong Kong and South Korea both introduced electronic wristbands paired with smartphone apps to enforce quarantine: if you left your home, the system would automatically alert authorities . Australia went a step further by trialing facial recognition for remote quarantine checks. In 2021, Australia’s two largest states began asking people in home quarantine to respond to random check-ins by sending a selfie through an app; an AI-driven system verifies the person’s face and location, and if either fails, police are dispatched . “You can’t have home quarantine without compliance checks,” argued the CEO of the software company providing this service, noting that manual checks simply couldn’t scale . Here again we see algorithmic enforcement: an app decides whether you are where you’re supposed to be, and flags you for police follow-up if not. This blurs the line between voluntary public health measures and police action initiated by an algorithm.

Across liberal democracies, softer forms of algorithmic rule enforcement also took hold. Digital contact tracing apps – deployed in countries from Singapore to Switzerland – would automatically notify users to isolate if data showed they were exposed. Some jurisdictions considered making such apps quasi-mandatory by tying them to access: e.g. requiring a green status on an app to enter certain public spaces. Automated temperature screening cameras became common at entrances, turning the public health advice of “if you have a fever, stay home” into an enforced rule – the door simply won’t unlock if the camera reads your temperature as high. In these ways, compliance was increasingly ensured by machines. The law (be it a health guideline or an emergency decree) was embedded in code and sensors, running continuously.

AI Enforcement and “Digital Police”

Alongside algorithmic rules, we witnessed the rise of AI enforcement – the use of artificial intelligence to detect violations and trigger sanctions in real time. The pandemic provided a pretext to roll out technologies that had been brewing in the tech world, from computer vision to biometric tracking, now repackaged as pandemic-fighting tools.

Consider the humble mask mandate. Enforcing mask-wearing for millions is daunting if relying on human officers. In 2020, several cities and transit systems turned to AI-powered camera systems to monitor mask compliance. In Paris, the transit authority RATP teamed up with a startup to install smart cameras in stations that could automatically detect how many passengers were wearing masks . The stated goal was statistical – “assess the proportion” of mask-wearers – but the privacy watchdog CNIL warned in May 2020 that even this pilot risked “generalizing a feeling of surveillance among citizens…detrimental to the proper functioning of our democratic society” . The French experiment was paused amid these concerns , illustrating an important point: the technology to automate compliance existed, but its use raised profound civil liberty issues. Still, the mere fact such AI surveillance was introduced in a Western democracy’s capital shows how normalized it was becoming to use AI for public order.

Other examples abound. Drones equipped with loudspeakers buzzed over parks and beaches in the US, Europe, and China, broadcasting messages to disperse gatherings . In some cases, drones used computer vision to spot groups or individuals violating lockdown – essentially robotic sentinels enforcing distancing rules. Police departments in California and New Jersey deployed drones to relay social distancing instructions, a practice critics blasted as “dystopian” . Thermal imaging AI cameras proliferated at workplaces and airports to flag anyone with elevated body temperature for further screening . And underpinning many of these tools was the expansion of facial recognition.

Facial recognition deserves special mention. Prior to COVID, its use was already growing (often quietly) in law enforcement and commercial settings. The pandemic supercharged it. Because it enables contactless identity verification, agencies found new excuses to deploy it at scale – from verifying unemployment benefit applicants in the US to ensuring the right person is quarantining in Australia . In the United States, at least 27 state unemployment offices rushed to integrate face recognition (via a service called ID.me) to authenticate claims when jobless numbers surged . The intent was to prevent fraud in distributing COVID relief funds. But this “AI enforcement” had side effects: many legitimate applicants were wrongly rejected by the algorithm and left without aid . Critics noted that errors in facial recognition disproportionately impact people of color , raising equity concerns when such tech becomes a gatekeeper for social services. More chilling, digital rights advocates pointed out that if this technology works as intended and becomes ubiquitous, it could be even more dangerous – enabling a normalized infrastructure of automated identification “everywhere… in stores… on public transit… in job interviews” . In other words, the pandemic was seeding a future where showing one’s face to a camera could be the equivalent of showing one’s ID to a cop at every turn.

Nowhere was the synergy of AI and enforcement more apparent than China’s fully integrated surveillance network. By 2021, reports showed that China was folding its COVID tracking systems into its broader public surveillance . The State Council (China’s top administrative body) explicitly planned to retain the pandemic big-data systems for long-term monitoring . What began as health monitoring was becoming a means to “patch gaps” in the surveillance state, making it more cohesive nationwide . Chinese authorities in essence treated COVID as a tech pilot program: successful new tools (like QR health codes, location tracking, mass facial recognition deployments to monitor crowds) would simply be kept and repurposed after the pandemic . This blurring of public health and public security mandates exemplifies what scholars label “function creep” – when a system built for one emergency quietly expands to other uses . Once millions are enrolled in a monitoring system, turning it off is often deemed “too risky” or a wasted opportunity by authorities. Absent strong legal sunset clauses, temporary measures can slide into permanent governance tools.

Vaccine Passports and the Rise of Digital ID Systems

If algorithmic law and AI enforcement were the sticks of pandemic governance, digital ID systems were the keys – the means by which compliance could be verified and managed at scale. During COVID-19, a person’s health status (tested? vaccinated? recently exposed?) became a critical credential. Governments and companies raced to develop “vaccine passports” or health passes, which soon evolved into embryonic digital ID platforms.

By mid-2021, dozens of countries had rolled out official digital certificates of COVID vaccination or negative tests. The European Union launched its EU Digital COVID Certificate, a scannable QR code available on paper or phone, which allowed cross-border travel without quarantine . Almost overnight, this system became the de facto passport for internal European movement and even access to domestic venues. France and Italy went further – requiring the pass not just for travel but for everyday activities. Italy’s Green Pass, for example, was initially a way to attend weddings or visit nursing homes, but it quickly expanded. By fall 2021, Italy mandated the Green Pass for all workers, public and private, effectively making proof of COVID status a condition for employment . Italians had to flash a QR code to enter offices, factories, trains, restaurants, gyms, even university classrooms . Those who lacked the pass (meaning unvaccinated or untested) could be suspended without pay after a short grace period , and faced fines if caught working regardless . Such sweeping use of a digital certificate system for population-wide regulation was unprecedented in a democracy. It essentially created a binary digital ID status – valid or invalid – that governed one’s ability to participate in society.

These COVID passes were digital ID systems in all but name. They authenticated an individual (often pulling from national ID databases to validate your identity and vaccination record), and they controlled access to services based on personal data. The World Health Organization even published technical standards for countries to develop interoperable digital vaccination certificates linked to identity, as a tool for both healthcare continuity and proof of status . In practice, what this meant was the emergence of a globally recognizable health ID – a template that could be expanded to other purposes. Tech experts noted that once you have a trusted digital credential on everyone’s phone, it could be extended beyond COVID – for example, to verify other vaccinations, or eventually as a general national digital ID for all government services . Indeed, initiatives were already underway by late 2021 to integrate vaccine certificates with national ID programs in some countries (and to incorporate fingerprint or facial biometrics for verification, as seen in China’s health code app linking to national ID numbers ).

Crucially, the infrastructure for these systems was built at lightning speed. Mobile apps, QR scanning procedures, backend databases – the pandemic jump-started digital identity projects that had lagged for years. The public, by and large, became accustomed to showing digital proof of identity and health to strangers – a security guard at a mall, a ticket agent at an airport, a receptionist at work. What would have sounded like a privacy activist’s nightmare in 2019 (i.e. “your personal health status will be required to enter a café”) became relatively routine in 2021. This compliance infrastructure relied on both centralized data and automated verification. For example, when someone scanned into a venue in France using the TousAntiCovid app, the system automatically checked the central database for vaccine validity. In some implementations, no sensitive health details were displayed – just a green check or red cross on the scanner. This was convenient, but it also meant the “decision” about your access was made instantaneously by an algorithm consulting a database. The guard at the door simply sees “Access Granted” or “Denied.”

From a governance perspective, this is transformative. Law enforcement by database query can happen anywhere, by anyone authorized with a scanner – not just uniformed officers. It creates a distributed enforcement network embedded in society. A restaurant owner becomes an enforcer of health regulations, empowered by a government app that tells them whom to let in. Some political philosophers and legal scholars began warning that this blurs public and private roles and could lead to outsourcing of enforcement to AI systems. What happens, for instance, if a future government requires a “social responsibility” certificate on that same app to access public places – perhaps to enforce carbon footprint limits or criminal background checks? The mechanism would be the same: digital IDs + automated permission checks.

Even outside of formal government programs, the pandemic saw rising adoption of digital ID verification for everyday transactions. Workplaces and universities implemented apps to verify test results or vaccine status for entry. Airlines collaborated on systems like CommonPass and the IATA Travel Pass to digitize health document checks. In many ways, COVID normalized that “your papers, please” moment in digital form, and it habituated the public to the idea that the phone in your pocket can serve as a universal ID – containing certificates, personal data, and a connection to government records at all times.

A Permanent Shift in Governance?

By the end of 2021, it was clear that these developments were not just one-off emergency measures, but a prototype of a long-term governance model. Policymakers and technologists spoke openly of applying the lessons of COVID to other areas: improving disaster response, streamlining government benefits distribution, combating future epidemics or even the flu. Underneath the optimistic framing was a reality – the architecture of control had been upgraded.

Governments now had far more ability to monitor and influence behavior in real time. National and regional authorities had rolled out integrated data systems that could track individuals (via phones or biometrics) across contexts. They had practical experience using AI to assist in governance tasks – whether allocating police to check on a flagged quarantine breaker or deciding who gets financial aid first. And importantly, a segment of the public had accepted that continuous surveillance and ID checks can be a “necessary trade-off” for safety.

To be sure, there was pushback and debate. Courts, privacy commissions, and civil society raised alarms. The French CNIL’s stark warning about smart cameras undermining democracy highlighted the risk of sliding into a surveillance society even with good intentions . In Singapore, public outcry erupted when it was revealed that police could access the supposedly private contact-tracing data, forcing the government to hurriedly pass legislation limiting such use . And in many democracies, digital health pass systems were explicitly temporary and set to expire when the pandemic ebbed. But the capabilities built – the expansion of surveillance tech and ID infrastructure – would not simply vanish. In China, as noted, authorities were unapologetic about keeping the COVID systems running for general security . Elsewhere, the door had been opened for a new kind of governance, one that some scholars later called the “Covid Technocracy”: a rule-by-data regime where human decision-making is augmented or even replaced by automated systems.

As we transition to the post-pandemic era, the question is not whether these systems will disappear (most will not), but how they will be governed and constrained. The experiment has demonstrated both the power and peril of algorithmic control. We’ve seen that AI can help manage a crisis at scale – imagine coping with millions of travelers’ vaccine checks without a digital system, or tracking infections without phone apps. But we’ve also seen how quickly these tools encroach on civil liberties if unchecked – the leap from contact-tracing to intelligence surveillance is frighteningly small, as Israel’s case showed .

The post-pandemic governance model that is emerging is a hybrid: part digital bureaucracy, part traditional authority. It leverages vast amounts of personal data (health records, location logs, biometrics), uses algorithms to flag non-compliance or risk, and issues directives (quarantine orders, access permissions) via digital means. It’s efficient – arguably more efficient at social control than any system before – but it tests the limits of democratic oversight. Without rigorous transparency, independent oversight, and “avenues for redress” as Freedom House urged , this model could morph into a stable apparatus of control that extends well beyond the pandemic’s needs.

Bold 2021 Prediction: By the mid-2020s, the “temporary” digital pass systems and AI surveillance tools deployed for COVID-19 will quietly evolve into permanent features of governance, effectively creating a world where one’s ability to move, work, or participate in society is controlled by ever-present algorithms checking a ubiquitous digital ID.

Chapter 7: The Psychology of Normalization – How Fear, Tech, and Convenience Reshaped Public Consent

Why did billions of people submit so readily to measures that, under normal circumstances, might have sparked mass outrage? Chapter 7 examines the psychological and social dynamics that made the extraordinary controls of the COVID-19 era not only possible, but in many places popularly accepted. A convergence of fear, technological dependence, and convenience created a powerful force for normalization – a process by which radical changes came to be seen as routine or even desirable. Understanding this process is key to recognizing how public consent can be engineered (or manipulated) during crises, and how temporary compliance can solidify into long-term acquiescence.

Fear as the Catalyst for Compliance

In early 2020, as a mysterious and deadly virus swept the globe, fear was pervasive. Fear of infection, fear for loved ones, fear of the unknown. That fear primed populations to accept stringent protections. Psychological studies during the pandemic found a clear link: individuals who felt greater fear of COVID-19 were more willing to comply with public health measures . Fear is a double-edged sword – it can motivate constructive action or blind people to potential overreach. Governments, whether intentionally or not, leaned into fear as a compliance tool. Daily death counts on TV tickers, emergency alerts on phones, and worst-case projections created a collective mindset that any measure, no matter how intrusive, was justified if it could save lives.

Public messaging often reinforced this. Leaders told citizens that draconian rules were the only alternative to catastrophe. In Italy, Prime Minister Giuseppe Conte implored Italians in March 2020 to accept a nationwide lockdown, effectively saying “there is no alternative if we want to protect our loved ones.” In the UK, the slogan “Stay Home, Protect the NHS, Save Lives” explicitly framed compliance as an act of altruism under dire threat. Fear appealed to a primal survival instinct and a social instinct to protect the community. When people are afraid, they are neurologically primed to seek safety over liberty. Decades earlier, after 9/11, a similar pattern was observed: fear of terrorism led the public to accept sweeping surveillance (Patriot Act, mass data collection) that would have been unthinkable before. The pandemic echoed this pattern on an even more global scale.

What makes pandemic fear unique is that it wasn’t just fear of an external enemy, but fear that everyone around you could be a danger (or you a danger to them). This created a level of social pressure to comply. If you disobey health rules, you’re not just risking yourself, you’re threatening others – so the fearful majority tended to socially sanction the non-compliant minority. In psychological terms, COVID risk turned compliance into a moral duty, enforced not just top-down but peer-to-peer. Many citizens became willing enforcers of norms: shaming neighbors who broke lockdown, filming strangers who didn’t wear masks, etc. Fear, when combined with moral fervor, normalized behaviors that border on vigilantism – but in this case aligned with state directives.

Surveys from 2020–21 showed surprisingly high support for even invasive measures. For instance, in a U.S. survey, over 70% of respondents supported stay-at-home orders and more than half even supported “centralized quarantine” facilities for infected individuals . Nearly 45% supported government monitoring of phones or wearables to ensure quarantine compliance . These numbers underscore how fear can tilt the scales: privacy and freedom were, for many, secondary to the immediate fear of disease and death. An April 2020 Pew Research poll likewise found most Americans prioritized controlling the virus over protecting personal privacy. In more collective cultures, like China or Singapore, the effect was amplified – fear fused with a sense of collective responsibility led to near-universal compliance with measures (a “we’re all in this together” mentality).

China’s case is illustrative: despite the intrusiveness of the health code surveillance system, multiple studies found that the Chinese public largely supported it because it was effective in containing the outbreak . The fear of COVID and the tangible results (low case numbers, quick return to near-normal life internally) \*\*strengthened public trust in the authorities and even boosted the legitimacy of the ruling party】 . When people are afraid, the promise of safety – especially if delivered effectively – can significantly increase tolerance for surveillance. The Chinese public’s attitude (“we accept being watched because it keeps us safe”) is a stark example of how normalization happens under fear: measures initially seen as extreme become viewed as prudent or even benevolent.

However, fear alone isn’t enough to sustain normalization. Human psychology has a way of adapting – what initially terrifies can become mundane as we grow accustomed to it. This is where technology and convenience came into play to lock in the new behaviors even after the initial fear plateaued.

Technology Dependency and the Comfort of the Familiar

By 2020, much of the world was already deeply entwined with digital technology. Smartphones, apps, and online services are integral to daily life. This existing technology dependence was a crucial substrate for normalization. The introduction of new surveillance or control measures often piggybacked on devices and platforms people already trusted and loved, softening their reception.

Think about contact tracing apps: instead of requiring people to carry a new government tracking device (which would have caused uproar), authorities released apps for your own smartphone – a device you feel in control of. It was framed as opt-in and as an extension of tools you use everyday. The familiarity of an app interface, the ability to download it from Apple or Google’s well-known app stores, and the integration with phone notifications all made the experience feel normal, even banal. “It’s just an app that sends me an alert – no big deal,” one might think, glossing over the fact that this app effectively knows one’s movements or contacts. Technology design here acted as psychological cushioning.

Moreover, the population was already conditioned to trade privacy for convenience in the digital economy. We click “I agree” on data-sharing terms of social media and map apps without a second thought, in exchange for useful services. The pandemic measures, in many cases, exploited this conditioning. Scanning a QR code at a restaurant to log your presence doesn’t feel wildly different from scanning a code to see a menu (a practice that also boomed during the pandemic). Showing a digital health pass is akin to boarding a plane with a digital boarding pass – a habit millions had already learned. Each step of compliance was often introduced as a technologically sleek solution, with user-friendly design. This emphasis on convenience and seamless tech integration was key to public acceptance.

Governments and companies made conscious efforts to highlight the convenience factor: “Skip the lines with digital vaccine proof,” “Use our app for faster entry,” etc. People who might object to carrying papers or being stopped by police were less bothered when the “papers” were just a phone app they tap at a turnstile. Convenience can be psychologically disarming – it reframes compliance as an easy, even pleasant experience rather than a burdensome duty. During the pandemic, many even demanded such tech solutions, frustrated with old-school bureaucracy. For example, when vaccine rollouts began, the public in many countries clamored for digital vaccine certificates to avoid having to carry flimsy paper cards. What started as a public health record quickly took on the features of a consumer tech product – complete with FAQs about app compatibility and how to retrieve your QR code if you lost it.

Another aspect of technology that fueled normalization is the perception of precision and impartiality. There’s a common public perception that computers and algorithms are objective and efficient. So when an app tells us to quarantine because of an exposure, we are somewhat more likely to accept it than if a human tracers told us – we assume the data is correct, the Bluetooth signal doesn’t lie. (Even though in reality, there were plenty of errors and false alarms in digital contact tracing.) This faith in technology’s accuracy made people more willing to trust algorithmic judgments. Similarly, seeing temperature kiosks or robot cleaners in public spaces gave people a sense of high-tech reassurance. The aura of technology – what might be called the “tech halo effect” – boosted confidence in the measures, which in turn encouraged compliance and normalization. In essence, technology provided not just tools but also a narrative of progress and control: we have smart apps and AI on our side, so we can beat this virus – and if that requires some surveillance, so be it.

Social media and the internet ecosystem further accelerated normalization. As millions posted pictures of their vaccination stickers or green pass on Instagram, compliance became a social norm celebrated online. App stores highlighted exposure notification apps as civic tools. The very rapidity with which these systems spread across countries gave people the sense that “this is just how things are now everywhere.” Observing that dozens of other nations were doing similar health passes or apps created a bandwagon effect – compliance measures felt less like an aberration if they were visible globally.

Convenience Versus Rights: The Subtle Trade-off

While fear drove initial acceptance and technology eased the process, convenience helped lock in new expectations. Consider how the narrative shifted: early on, a COVID pass was sold as a way to safely restore freedoms (e.g., “with this pass, you can travel or dine out again”). The pass was an extra step, yes, but one that made life more convenient under restrictions. Over time, this flipped – people began to expect that showing credentials was a normal price of admission. By late 2021, surveys in countries with health pass systems showed majority support for maintaining them at least until the pandemic’s end, and significant minorities open to using them for other vaccinations or future outbreaks. The inconvenience of occasional QR scans was normalized because it was offset by the convenience of keeping society open. In psychology, this is akin to classical conditioning: we associated these new behaviors with positive outcomes (safety, open restaurants, travel), rather than just with the negative of being controlled.

Yet, beneath the surface, there was a trade-off: convenience was often achieved by centralization and data sharing, with implications for privacy and autonomy. But the public discourse downplayed those concerns. In part, this was because convenience speaks to immediate personal experience, whereas privacy invasion is an abstract or deferred harm. For many, the mindset became “if I don’t feel harmed right now, then there is no harm.” Scanning a pass takes seconds and I’m on my way – it doesn’t feel like a rights violation the way an overt police checkpoint might. This psychological distancing from the potential abuse of these systems made it easier for people to consent.

Authorities and businesses also learned to frame measures in terms of choice and personalization, even when they were essentially mandatory. For example, if a country required either vaccination or frequent testing for workers via a digital pass, it was framed as giving people options – you choose how to comply. This sense of choice, however constrained, can preserve a feeling of autonomy, which makes people less resistant. At the individual level, many rationalized: “I chose to get vaccinated and use the pass, it’s my decision to protect others.” That internal narrative is far more palatable than “the government is forcing me,” even if functionally both lead to the same outcome of widespread compliance.

Normalization set in gradually. What was once shocking becomes expected. After months of lockdowns and travel bans, people were grateful to be allowed to do things with a pass – so showing the pass became second nature. Psychologists call this habituation: repeated exposure to a stimulus (in this case, surveillance or ID checks) reduces our emotional response to it. By 2021, a commuter scanning a code to board a train felt it as routine as swiping a transit card. A student logging daily symptoms into a campus app became just another morning chore. Over a period of time, entire populations were effectively trained in new behaviors by repetition.

Importantly, public discourse began to shift from “if” to “how” these measures should be used. Early in the pandemic, debates raged: Should we accept digital contact tracing? Should we have immunity certificates? Those were debates about if society should go down that road. But once implementation began, the debate largely shifted to how to do it properly: how to protect privacy in apps, how to ensure equitable access to passes, etc. While these discussions were vital, they also signaled a tacit public consent to the premise of these systems. It was no longer a question of acceptance, but of fine-tuning. This is a hallmark of normalization: the baseline has moved.

The media also contributed. After initial novelty, coverage of surveillance and pass systems became more matter-of-fact. The extraordinary became ordinary in news storytelling. For example, a headline in mid-2020 might have read “Controversy as Government Tracks Phones to Enforce Lockdown”; by mid-2021 it was more like “To Travel, Upload Your Vaccine QR Code – Here’s How.” The tone shifted from alarm to instruction. In democratic societies, some investigative reporting did keep spotlighting abuses (like police misuse of health data, or data breaches of tracing apps), but these were often seen as isolated problems to fix, not reasons to dismantle the overall apparatus.

The New Social Contract of Convenience

What emerged was a kind of new social contract, driven by both fear and convenience: citizens agreed to visible constraints and data sharing in return for the promise of safety and the partial return of their pre-pandemic lives. Public consent was not so much explicitly given (few places held referendums on these issues) as it was manufactured by circumstances. It’s a phenomenon political scientist Naomi Klein and others dub the “shock doctrine” – crises create an opening for rapid changes that people might resist under normal conditions. In this case, the shock (the pandemic) enabled a leap in surveillance and control, and the normalization process sealed it by making those changes feel acceptable and even commonsensical.

However, one must note that consent was not universal or uniform. There were protest movements – from anti-lockdown rallies to civil liberty lawsuits – in many countries. Some people never adopted the apps or resisted the passes (with consequences like losing jobs in some cases, as in Italy’s Green Pass scenario ). The psychology of normalization did not enchant everyone. But a combination of majority acquiescence and fatigue marginalized the opposition. Many who initially had misgivings felt social pressure to go along, not wanting to be labeled as irresponsible or “one of those conspiracy theorists.” Over time, even skeptics often begrudgingly complied out of necessity or social harmony. This is another psychological facet: the need to belong and not be ostracized. In an environment where the mainstream embraced the new rules, being the odd one out became harder.

We also can’t overlook the role of trust in authorities and experts. In places where governments communicated clearly and demonstrated competence, people’s trust increased and they were more willing to accept guidance, even if it infringed on privacy. For example, public trust in scientific and health authorities was a strong predictor of willingness to use contact tracing apps and comply with rules . The converse was true: where trust was low, compliance was more grudging and fragile. But globally, the initial success of harsh measures in suppressing the virus (e.g., China’s early lockdowns, New Zealand’s isolation strategy) served as proof to many that strict measures work, thus justifying their own acceptance. It’s a psychological reinforcement loop: compliance leads to better outcomes, which reduces fear and proves the value of compliance, which in turn makes continued compliance more likely even as fear subsides.

By late 2021, much of the world had adapted to a reality that would have seemed outrageous two years prior. Children were used to seeing everyone in masks; adults were used to flashing personal data to enter buildings; families were used to the idea that the government might track their location if needed for public health. Through fear, we leaped into these behaviors, and through convenience and habit, we stayed.

The long-term danger in this psychology of normalization is subtle. When the next justification comes – it could be a new variant, a different public emergency, or something less acute like a rise in crime – societies now have a precedent of broad public acceptance for heightened surveillance and control. Each time we normalize a loss of privacy or freedom, it becomes harder to make the case to undo it. The generation that comes of age in this environment may not even perceive what was lost. A college freshman in 2021, for example, might find it normal that the university app tracks their movements “for safety” and will carry that expectation into the wider world.

Yet, understanding this process also reveals potential points of intervention. Public consent is malleable. It was shaped by narratives of fear and convenience – it could also be reshaped by narratives of rights and empowerment. Normalization can be countered if enough people recognize what is happening and recall that “normal” is not always synonymous with “good.” In 2021, these patterns were still playing out, but to someone tracing the system’s evolution, the direction of travel was clear.

Bold 2021 Prediction: Fueled by the crisis, societies have crossed a threshold: by the mid-2020s, people will accept routine surveillance and digital checks as “just part of life,” largely forgetting how extraordinary these powers once seemed – a psychological permanence born from temporary fear.

Chapter 8: A Final Warning and Vision — What AI-Powered Control Could Become by 2030 If Decentralization Fails

Looking ahead from the vantage point of 2021, one can glimpse two starkly different futures. Down one path, the world learns from the COVID-19 experiment and reins in centralized control, building more decentralized, privacy-preserving systems for the public good. Down the other path – the path of least resistance – the temporary measures solidify into a permanent AI-powered apparatus of control. In this final chapter, we offer a warning and a visionary projection of what could await by 2030 if we collectively fail to course-correct. The pandemic has shown the blueprint of a high-tech authoritarianism that doesn’t require a dictator in the classical sense, but rather grows out of the seamless integration of surveillance technology into governance. If decentralization of power and data is not achieved, by 2030 we may find ourselves living in a world that makes the writings of Orwell or Huxley pale in comparison.

2030: The Fully Algorithmic Society

Imagine it is 2030. The vestiges of the COVID-19 pandemic are long past, but its digital infrastructure remains – expanded and repurposed. Every citizen is now tagged with a universal digital ID, which evolved from the vaccine passports and national ID programs of the early 2020s. This ID is required for virtually all transactions and interactions: not just travel or entering buildings, but logging onto the internet, accessing financial services, receiving healthcare, and even voting. It is tied to a unified ledger of personal data: health records, educational and employment history, travel logs, social media profiles, and a continuously updated behavior score.

In 2030’s daily life, AI algorithms pervade decision-making. Perhaps you hail an autonomous taxi; as you enter, a camera scans your face and verifies your ID, linking to your account – if your “mobility privileges” are in good standing, you are whisked away. What could affect those privileges? Maybe a recent lapse in bill payments (since digital currency is now programmable, missed payments can flag your ID), or perhaps last week you were near a protest that police deemed unlawful. In a fully algorithmic society, the rules are encoded and enforced automatically at every step. No human need directly confront you; the system simply knows and acts. This is an extrapolation of what we saw in 2020–21: health codes dictating movement , only now the criteria extend beyond health.

By 2030, if decentralization fails, national and corporate databases may well be integrated globally. We could see the emergence of something like a Global Citizen Profile managed jointly by governments and perhaps big tech consortia. During the pandemic, we saw international systems like the EU COVID Certificate and proposals for WHO-backed global health passes . In a dark 2030 scenario, this interoperability extends: your country’s system seamlessly shares data with others as a condition of travel or trade. Cyber sovereignty – the idea of each nation controlling its internet and data – might give way to a new reality where bloc-based or global networks standardize citizen monitoring . If Western democracies follow the path set by more authoritarian regimes in embracing surveillance tech, by 2030 there may be little practical difference in how closely citizens are watched in Beijing, Washington, or London – only a difference in how it’s justified.

AI-powered control means that the sheer volume of data gathered (from billions of IoT sensors, cameras, and digital activities) is analyzed and acted upon by machine learning in real time. This enables what one might call “predictive governance.” For example, rather than waiting for a crime to occur, algorithms predict hotspots of social unrest or rule-breaking and preemptively restrict certain people’s movement or communications. In 2021 this was speculative, but even then, elements were present: China’s systems already attempted rudimentary risk scoring for individuals’ COVID exposure , and police in some countries started using predictive policing algorithms for crime. By 2030, without intervention, these could fuse. An AI might flag a person who frequently visits online forums critical of the government and also attended a political rally, marking them as a potential “troublemaker.” Their digital ID might silently get a note that triggers extra scrutiny whenever they make large purchases or try to organize gatherings (detected through messaging apps that are no longer end-to-end encrypted, since governments mandated “lawful access” backdoors around mid-decade).

In this future, the idea of privacy as we knew it in the 20th century is extinct. Continuous surveillance is the norm: streets are lined with smart cameras; drones patrol public events; your home’s smart appliances report usage patterns to the cloud (nominally for energy efficiency, but the data is accessible to authorities under broad “public safety” laws). People adapt their behavior, knowing they’re watched. Most don’t feel oppressed day-to-day, because it’s been normalized (as we explored in Chapter 7). It’s simply how society functions – the price of safety and convenience. Dissent becomes more self-censored; the chilling effect of possible surveillance silences many before they even speak.

Notably, such a system may not feel overtly tyrannical on the surface. There might be no jackbooted troops on every corner. Instead, control is silently exerted via algorithms. If you deviate from expected norms, you get an automatic push notification from a government service: maybe a polite reminder to attend a “health and safety re-education seminar” because your risk profile spiked. Or your bank app pops up a warning that your spending this week is unusual and could violate some policy. The enforcement is often just a denial of service: you can’t buy a plane ticket because the system doesn’t issue you the required authorization QR code; you can’t post certain ideas on the dominant social platforms because an AI filters your content (something already well underway in 2021). Censorship and control blend into the background of everyday tech.

Perhaps one of the most far-reaching developments by 2030 would be the widespread introduction of central bank digital currencies (CBDCs) fully integrated with digital IDs. In a centralized scenario, this means every transaction you make is recorded and can be approved or declined based on compliance with rules. During COVID, governments learned they could direct behavior with stimulus payments and fines. In 2030, with programmable money, if you violate a rule your digital wallet could be docked a penalty instantly. Or certain funds could be made to expire or be restricted to certain uses (for instance, a climate initiative might restrict how much gasoline you can buy per week, enforced via currency that simply won’t transact beyond the allotted amount). This is not sci-fi; central banks were openly discussing such capabilities in 2021 and beyond. Without decentralization, the risk is that such powerful monetary control tools become another layer of the surveillance state.

By 2030, the consolidation of data and power might reach a tipping point: a permanent state of exception. We would live under what some theorists call “the security paradigm,” where virtually any issue (health, environment, terrorism, misinformation) is managed through the apparatus of surveillance and control built originally for the pandemic . We already saw the rhetoric in 2020: leaders talking about “war” on the virus. In the following years, that rhetoric could shift to a “war on climate change” or responding to “infodemics” of misinformation – all possibly used as justifications to keep the sensors rolling and the AI monitoring tuned on high. Essentially, emergency logic could become permanent governance logic.

The Cost of Failing to Decentralize

All of this paints a grim picture, but it is a plausible one if current trajectories continue unchecked. The root problem is centralization – of data, of decision-making, of authority over technological systems. In 2021, there were already voices warning that we must decentralize: for instance, proponents of decentralized contact tracing (using Bluetooth exchanges stored on user devices rather than central servers) argued it was possible to get public health benefits without building giant databases . Similar arguments were made for self-sovereign identity – digital IDs that individuals control rather than governments – and for open, transparent algorithms rather than black-box AI. If those advocating for such designs do not succeed, the likely alternative is the one described above.

The cost of failing to decentralize can be summarized in a few key dangers:

• Loss of Individual Autonomy: When every action is tracked and can be nudged or sanctioned, the capacity for individual choice outside the approved norm diminishes. Free will becomes constrained by an invisible cage of algorithmic predictions and prescriptions.

• Abuse of Power: As Edward Snowden famously noted, any system of total surveillance will eventually be misused. We saw glimmers of it when some governments abused contact-tracing data to monitor dissidents . By 2030, a fully centralized system would tempt whoever controls it – be it authoritarian regimes or even democratic governments during crises – to use data against political opponents, minorities, or activists. Without decentralization or robust checks, the technical ability to abuse will sooner or later meet the political motive to abuse.

• Inevitability of Errors and Omission of Redress: Complex AI systems are fallible. They will make mistakes – accusing innocent people, misidentifying threats. In a centralized regime, contesting these errors is hard. We saw people wrongly flagged by facial recognition unable to get their unemployment benefits until the media intervened . In 2030’s scenario, if your “social credit” drops due to an AI error, you might be stuck in Kafka-esque digital limbo with no human officer to appeal to. Decentralization of data and power can provide safety valves – multiple sources of truth, local autonomy, and human oversight – but without it, errors can become life-altering and nearly impossible to overturn.

• Homogenization of Society: A less discussed effect – when algorithms enforce norms, societies risk losing the diversity of thought and behavior that drives progress. If by 2030 everyone’s choices are nudged toward some algorithmic average of “acceptable,” creativity and dissent suffer. Already, recommendation algorithms on social media create echo chambers; extend that to life choices and you get a subtle form of algorithmic conformity.

So what does decentralization mean in this context, and why is it the antidote? It means distributing data storage and decision power away from single central authorities. For instance, instead of one centralized health surveillance network, we could have local systems that federate when needed, sharing only minimal necessary info (as some privacy-by-design systems attempted). It means giving individuals more control over their digital identity and how data about them is used. Technologically, it might involve blockchain or other distributed ledger technologies to ensure transparency and reduce single points of failure or control. Socially, it means reaffirming principles of subsidiarity (decisions made at the most local level feasible) and strengthening democratic oversight of any technology that affects rights.

The vision of 2030 we want is one where the tools developed in the pandemic are repurposed for empowerment, not oppression. For example, imagine a world where health data is kept on personal devices under the individual’s control, only shared in anonymized aggregates for research – that’s a decentralized approach that contrasts with central databases. Or a world where AI algorithms that influence public life are required to be open source and vetted by citizen panels for bias and fairness. Or where critical infrastructure like digital currency has built-in privacy protections (like digital cash) rather than total traceability.

In 2021, these ideas were gaining traction among technologists and civil libertarians, but they faced an uphill battle. Governments and large corporations often prefer central control – it’s efficient, and it preserves their power. Decentralization can sound messy and threaten the tight grip of authorities. Yet, if the warning signs from the COVID era are heeded, there might be broader support for decentralization as people realize what’s at stake. Freedom House, for instance, warned that responses to the pandemic were “laying a foundation for tomorrow’s surveillance state” and urged policies to foster a “reliable and diverse information space” – essentially calling for decentralization of the internet and information flows to counter the authoritarian trend.

The coming years (2022–2025) are pivotal. They will determine whether we bend the arc toward decentralization or stay on the centralized path. If we stay the course without corrections, by 2030 the scenario described – or elements of it – will manifest. We can already see early signals: the spread of China’s surveillance exports to other countries, the way some democracies are quietly expanding legal justifications for data collection, and how tech firms are eager to monetize centralized health and identity systems.

This chapter is not a fatalistic prophecy but a conditional warning. The future is not written in stone. In the aftermath of the pandemic, society has a brief window to reflect: which parts of the emergency apparatus do we dismantle, which do we keep, and under what governance? Strong advocacy for privacy and decentralization now can prevent the worst outcomes. For example, pushing for laws that delete or anonymize COVID-era data (as some proposed, to avoid “function creep”) , or implementing “sunset clauses” that ensure extraordinary powers expire and require new public debate to extend.

Yet, if such measures fail and decentralization stalls, we must be prepared for a reality where AI-driven control is the default. In that world, personal freedom will depend less on legal safeguards and more on technical ones – meaning if the tech is designed to control, it will be very hard for individuals to escape it. The disparity between those who control the AI infrastructure and those who live under it could widen, creating a new kind of class system: the watchers and the watched.

Bold 2021 Prediction: Absent a decisive shift toward decentralization, the late 2020s will see the rise of a global technocratic order – a system where unelected algorithms and centralized data define our lives, and where personal freedom survives only at the margins or behind encryption – eerily validating the warnings of 2021 as today’s unfolding reality.