Universiteit
Leiden
The Netherlands

A Critical Analysis of the Progressive erosion of Privacy Rights: A Cross-Case examination of COVID-19 and the eID

Diephuis, Christina

Citation
Diephuis, C. (2023). *A Critical Analysis of the Progressive erosion of Privacy Rights: A Cross-Case examination of COVID-19 and the eID*.

Version:	Not Applicable (or Unknown)
License:	License to inclusion and publication of a Bachelor or Master thesis in the Leiden University Student Repository
Downloaded from:	https://hdl.handle.net/1887/3633840

Note: To cite this publication please use the final published version (if applicable).

A Critical Analysis of the Progressive erosion of Privacy Rights:

A Cross-Case examination of COVID-19 and the eID

Master's Thesis International Relations: Global Order in Historical Perspective

Faculty of Humanities

Word Count: 13646

Student: Christina Diephuis. S2076063

Supervised by Stacey Links

February 20, 2023

Universiteit Leiden
The Netherlands

Table of Contents:

Acknowledgments:

I would first like to thank my supervisor for her feedback. Second, my family and friends for their moral support. Lastly, my friend Sorcha for spending some of her valuable time proofreading my thesis.

I. Introduction

Historical Background

Human rights emerged after the horrors of World War II, among which Nazi eugenics laws purported a public health justification of "healing the state," massively violating the 'rights' of minority populations (Sekalala et al. 2020, 10). Here, international leaders reunited to discuss rights that everyone would be entitled to have. Nevertheless, intelligence agencies have battled the universal right to privacy possibly since its inception in 1948 with the Universal Declaration of Human Rights (UDHR), although the consequences of this violation are perhaps most vivid today. Article 12 of the Universal Declaration of Human Rights (UHRD) explains the protection of the universal right to privacy as:

> "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to legal protection against such interference or attacks" (United Nations General Assembly 1948).

The first intelligence collection and mass surveillance efforts arguably began in 1946 with the Five Eyes Alliance, a secretive, English-speaking, global surveillance network of states (Pfluke 2019, 304). The Alliance consisted of a United Kingdom (UK) - United States (U.S.) Communication Agreement of intelligence sharing, created to contain potential threats from the Soviet Union (ibid., 302). In 1952, the National Security Agency (NSA) was launched, helping centralize all communications intelligence and creating a foreign signals intelligence (SIGINT) empire in the U.S. (ibid., 304). According to NSA, SIGINT is used to save lives, defend the US, and advance U.S. principles and alliances globally (NSA n.d.). Moreover, it gathers information about persons, international terrorists or foreign powers, and organizations (ibid.). Thus, a form of arbitrary interference with people's privacy. In 1956, the Alliance expanded to include Canada, Australia, and New Zealand. With the Five Eyes, a worldwide surveillance program for collection and analysis technologies called Echelon was created (Pfluke 2019, 302). However, only in 1999 did the head of the Australian Defence Signals Directorate (DSD) become the first person to openly admit their country's involvement in the global surveillance alliance and Echelon (ibid., 304). Moreover, while surveillance and the collection of identity intelligence could be relevant to find crime suspects, it is unclear whether it is proportionate and fair, to implement the same approach to every individual.

The terrorist attacks of September 11, 2001, in New York, were followed by the proclamation of the "Global War on Terror" by American ex-president, George Bush. This marked another decisive historical period that legitimized further intelligence collection activities to combat terrorism (Kleining et al. 2011, 130). In 2013, a former NSA member, Edward Snowden, shed light on the abusive role of the NSA organization in intelligence collection and unnoticed intrusion on citizens by abusing their power to access civilian webcams and to record. Also, Snowden advanced that the NSA had been using mass surveillance (also called strategic intelligence) to interfere in mass communications rather than tracking solely crime suspects, creating a permanent profile of every American (Snowden 2019, 8). Snowden's confessions led to policy reforms and attempts to rebuild public trust in intelligence services and the NSA (Mansfield-Devine 2013, 5). However, the whistle-blower was not praised for his efforts to defend human rights. Instead, he had to seek asylum in Russia, still faces international persecution, and an imprisonment order was brought against him for violating the 1917 Espionage Act (Amnesty International UK 2020). The NSA has never officially apologized, or has been held accountable for their illicit, yet purposeful involvement in citizens' privacy. On March 11, 2020, the WHO declared the COVID-19 pandemic (Murphy 2020, 495), after the first detection of the virus SARS-CoV-2 was found in November 2019 in Wuhan, China. This event was followed by the introduction of drastic illiberal measures to combat and control the virus, implemented on a global scope. Namely, quarantine enforcement, social distancing, lockdowns, and technology-based solutions like contact tracing apps, and in 2021, digital COVID Certificates with Vaccination or recovery status, and occasionally a test result, for traveling and entering establishments (Kitchin 2020, 363). Nevertheless, the advances in identification have been progressive, at least in the EU, with the prospect of 100% of key public services being made available online by 2030, as well as e-health, and the launch of the European Digital Identity or eID by the EU Commission which is expected by 2024 and held by 80% of Europeans by 2030 (European Commission n.d.).

Given the historical progression of mass surveillance eroding privacy rights, this thesis presents the following critical research question:

How do policymakers increasingly justify policies that erode privacy, and how are these prejudicial to other human rights?

This thesis answers this research question through the cross-case study of COVID-19 (2019-2022) and the eID in the EU, which sheds light on how policymakers used the event to justify

and introduce long-term policies, and their potential effects on human rights. Namely, European digital identity, which throughout this thesis will be referred to as the eID.

Relevance and research objectives

The right to privacy is perhaps one of the most disregarded human rights from the UDHR, and its relevance to other human rights is often overlooked. Several authors have argued that the lack of interest in sharing liberal values of autonomy and privacy, are characteristics of authoritarian states (Kleining et al. 2011), making privacy a relevant public policy concern to examine in International Relations. Given the novelty of the COVID-19 pandemic, this case was chosen to explore whether this event enhanced policymakers' justification of surveillance and the erosion of privacy rights. This case study may also contribute to the public health surveillance debate, rising from COVID-19. This will be conducted by critically examining the legitimacy of this 'cross-border threat', and whether its digital countermeasures were set to prevail through the eID. Testing the hypothesis presented by Farrell and Newman (2019) on the transatlantic struggle between privacy and security. Lastly, authors like Marciano (2018), have stressed the need for connecting technical and social sciences, as social scientists are unlikely to delve into technicalities, and engineers rarely take on critical humanities or social research (133). Hence, this thesis would also contribute to enhancing conversation between these fields, suggesting a human right-oriented perspective to the eID, fueled by the examination of COVID-19, and its countermeasures' impact on human rights.

Overview

Chapter II, the literature review, explores the contestations of privacy rights, re-addressing the relevance of this right as discussed in academia, and perceptions of this right by different actors. Then, Chapter III, methods, illustrates the methodology used for the collection and analysis of the information present in this dissertation, as well as the theories used for the cross-case study interpretation. Chapter IV constitutes a substantial chapter that provides additional background on the ongoing debate of current communications and biometrics surveillance mechanisms in Western countries. Additionally, this chapter contributes to the final Human rights legal interpretation that precedes the discussion. Chapter V de-constructs COVID-19 through the theoretical approaches introduced in the methods chapter, Securitization theory, Agenda-Setting and Framing, and the Human rights framework. Then, it tackles the question of whether COVID-19 served to introduce the eID in two sub-chapters.

Here, this thesis provides the last human rights legal concerns arising from COVID Countermeasures and the European eID. Lastly, this thesis concludes by outlining its contributions and research limitations.

II. Literature Review

This literature review revisits scholars' interpretations of the perceptions of privacy in different sectors, namely within the legal sector, academia, society, big tech, intelligence, and public health. These approaches were identified when investigating the literature on the justifications used for mass surveillance, which directly correlates to the violation of privacy rights. Understanding these attitudes towards privacy is critical to explaining the relevance of protecting privacy rights and why these perceptions raise concerns as to how COVID-19 could have been used, or abused, to accelerate further policies.

The legal, academic, and public meaning of Privacy Rights

Although privacy advocates have played a major role in fighting surveillance to defend privacy rights, there are pressing issues in the definition of privacy that delimit the protection of privacy rights. According to Burt (2019), U.S. Supreme Court Justice Louis Brandeis (1916-1939) defined privacy as "the right to be let alone" (17). Moreover, Scanlon (1975) describes the most evident form of 'offensive intrusion' or privacy violation, as the "observation of our bodies, our behavior or our interactions with other people, or overhearing of the last two" (315). However, neither the U.S.-nor the Canadian Privacy Acts define "privacy" (Flaherty 1986, 13). In addition, the lack of public interest also contributed to the reluctance of the government to revise the Privacy Act of 1994, despite its numerous deficiencies (Flaherty 1986, 8). However, Flaherty (1986) argued that legislators and academics never provided a consistent definition of privacy (13), which up until today is still an issue. In academia, several authors have attempted to define privacy. Moore (2008) for example, argues that privacy is difficult to define universally, because "rituals of association and disassociation are culture and species related" (411). Similarly, Acquisti et al. (2016) argue that what constitutes sensitive information like unemployment, health status, and criminal record, differs across individuals (446) making privacy questions non-universal but context and individual-dependent. Yet, Burt (2019) takes

a different approach to privacy, arguing that privacy today is the ability to "control data we cannot stop generating, giving rise to inferences we cannot predict" (17). This perception of privacy has certain limitations, as it concerns mainly the protection of data provided to machines and collected through internet "cookies", for example. Still, this definition has gained momentum since, similarly, Acquisti et al. (2016) defined privacy as control over sharing (445). Also, as cited in Marciano (2019), "the most common definition of privacy is the ability of individuals to control their personal information (Westin 1967; Altman 1977; Rule 2012), and scholars usually frame this harm as a "privacy violation" (129). Other authors have also addressed privacy as "an aspect of dignity, autonomy, and ultimately human freedom" (Schoeman 1992) (as cited in Acquisti et al. 2016, 443). Ultimately, these definitions have significant limitations, so perhaps a combination of all their aspects as well as the views by Louis Brandeis and Scanlon (1975), would make a definition of the right to privacy more complete.

Privacy concerns first arose as a public policy issue in the 1960s (Bennett and Raab 2020, 448) when mass surveillance projects raised citizen concerns among citizens regarding their potential nefarious purposes, which ranged from discrimination to political control (Flaherty 1986). Bennett and Raab (2020) also claim, like Flaherty (1986) that the way privacy protection debates are solved today will have far greater implications for global communications, the flow of personal data, and the internet (461). There is a worrying ongoing debate concerning current forms of surveillance. Marciano (2019) states that there has been a shift from voluntary information disclosure and sharing to its involuntary, automatic, or remote retrieval by "powerful others" (129). In a similar vein, Rusinova (2012) describes a phenomenon where being watched becomes a social norm, and individuals easily renounce their privacy for comfort, entertainment, or communication, raising questions as to why the individual's privacy should be protected (12). Also, leaving 'privacy resigned' due to the inevitability of consumer surveillance (Rusinova 2021, 8). In the same vein, Ribeiro-Navarrete et al. (2021) describe this as 'surveillance capitalism', where an individual's (bulk) data can be collected and exchanged, perhaps unconsciously, for the use of free applications (2). Sekalala et al. (2020) also address current trends of lessened privacy online, the profitability of online data, the utility of big data in policymaking, and governments' abuse of online surveillance (8). Similarly, the authors claim that these trends are creating "surveillance states" and new forms of "surveillance capitalism", as Ribeiro-Navarrete et al. (2021) also claimed, with the potential to erode human rights and undermine democracy (ibid.). Yet, authors like Kleining et al.

(2011) stress that expectations of privacy must change from the "sense of evanescence" that phone conversations used to have, given the storage of email, chat, and digital data by third parties today (134). Other authors have highlighted the relevance of privacy, as it serves as the foundation for other necessary human rights, like personal autonomy, and the freedoms of expression, association, and choice. Arguing that with its demise, other fundamental rights, and values "are sure to be asphyxiated by the invisible toxin of unfettered surveillance" (Lubin 2018, 526).

Big tech

In these new forms of surveillance capitalism, several authors have addressed the shifting power from governments and intelligence agencies to Big Tech companies, although they appear to hold questionable views toward privacy concerns. Csernatoni (2020) argues that Big Tech companies play an increasing geopolitical role, as companies like Google, Amazon, and Facebook have "unparalleled control over knowledge about individuals, groups, and society across borders" (306). Similarly, within this strain of corporate surveillance, Rusinova (2021) uses "personal data as a commodity" to describe the elusive character of the notice and choice system on the internet, given the increasing indispensability of the internet to perform essential activities (8). This somewhat forces the individual to trade personal information for information essential for daily tasks. Companies have also contributed to triggering the "the body as password" concept, which is used by surveillance scholars to address the role of biometrics as gateways to physical and virtual spaces (Marciano 2019, 1). For instance, through the introduction of biometrics to view all saved passwords, widely used by iPhone users. Perhaps the normalization of providing data without understanding the consequences has been the trigger to the "I have nothing to hide" public response to privacy questions, since they may rather trade privacy for comfort. This has also been termed "dataism", a phenomenon where the masses naively and unsuspectingly entrust their personal information to corporate platforms (Csernatoni 2020, 306). Authors like Acquisti et al. (2016) condemn these views, since they may legitimize expansions of intrusive surveillance programs that affect the rest of society (446). This has different setbacks, the most extreme exposing individuals to severe harm if becoming victims of identity theft (447), causing irreparable harm if biometric data is stolen. Mansfield-Devine (2013) addresses the government's inability to control the flow and replication of data (5) and that it is not clear what authorities are getting from internet

surveillance systems (11). Here, the author provides the example of Google, which uses Gmail messages to display personalized advertisements. Surprisingly, in a court case challenging this, the company defended itself by claiming that email users could not expect any privacy of the information they voluntarily give to third parties (Mansfield-Devine 2013, 6). This invariably poses critical questions regarding the security and trustworthiness of the devices and platforms where individuals allocate their data.

Governments and Intelligence agencies

According to several authors, governments and intelligence agencies hold very different views of privacy, in comparison to legal views on privacy. For instance, U.S. House Intelligence Committee Chairman Mike Rogers claimed that: "you cannot have your right to privacy violated if you do not know your right to privacy has been violated" (Lubin 2018, 525), meaning that if done secretly, it is not a privacy violation. Additionally, governments have used the "honest citizen" argument (Milone 2001, 508), and citizens have perpetuated it through the "I have nothing to hide" views, although this is vastly criticized by privacy advocates (Acquisti et al 2016, 446). Whether privacy could ever be achieved in the digital era remains a questionable issue, as Lubin (2018) claims that "intelligence agencies are from Mars, and privacy experts are from Venus, and the two could never meet" (551). Bernal (2016) also complains about the lack of transparency in data collection by intelligence agencies (258), which consequently erases the individuals' capacity to know and control who had access to, collected, analyzed, or shared their data. Nevertheless, Snowden stresses the relevance of this issue by stating that the freedom of a country can only be measured by its respect for its citizens' rights, limiting the government's power. Rather than liberty, as in the American Revolution, he states that during the internet revolution, this is called "privacy" (Snowden 2019, 11). Königs (2022) also critically argues that government surveillance might end up being used to enforce illegitimate laws and severe punishments for an infraction, as Snowden also advanced (14). Hence, turning extreme justice into extreme injustice due to the coercive and undefeatable power of government action (Königs 2022, 11). According to a report launched by the United Nations Human Rights Office (OHCHR) in 2014, government surveillance has emerged "as a dangerous habit rather than an exceptional measure" (Watt 2017, 784). Yet, the OECD Guidelines from 1981 state that the collection of personal data should have limitations and be collected and used only for purposes specified at the time of collection (Flaherty 1986, 8). Also, Watt (2017) claims that it should be illegal for intelligence

agencies to force telecommunication and internet companies to grant them access to bulk metadata without a court order (784).

In Europe, in 2016 a proposal called “Intelligence Codex” was launched to ban mass surveillance since it has been defined as unlawful. Nevertheless, it was refuted by the Dutch government, which viewed banning the state’s investigatory powers as unrealistic and irresponsible for intelligence collection (Watt 2017, 774). Strikingly, no other scholars were found to have written on the rejection of the Intelligence Codex. Within the field of international privacy rights, the subject does not seem to improve, as there is an ongoing contestation of asymmetrical privacy protection regimes, which violate the universality of privacy rights as human rights. The engagement of political leaders and political elites in programs of bulk interception, mining, analysis, and dissemination, also rises concerns since these are all susceptible to abuse and “impropriety” (Lubin 2018). Whenever these officers are confronted, Lubin (2018) claims that policymakers respond with a smile and claim “there is nothing you should worry about” justifying the use of these programs as only applying to foreigners and dismissing the importance of protecting their universal human rights (Lubin 2018, 508). Yet, with the existence of the Five Eyes, a global intelligence-sharing alliance, this justification only shows a lack of transparency which does not guarantee that other foreign intelligence agencies or corporations are not intercepting domestic’s privacy through their allies. Similarly, Cayford et al. (2018) interviews of intelligence policy officers vaguely exposed their engagement in bulk data collection and intrusion in communications, although with controversial explanations and no emphasis on the implications to privacy rights. Here they explain that intelligence agencies like the NSA and the CIA engage in two types of intelligence strategic and tactical or operational (Cayford et al. 2018, 93). While tactical intelligence targets a specific threat, strategic intelligence collects bulk data. In the case of tactical intelligence, security threats have been efficiently stopped, while controversially, the effectiveness of strategic intelligence is measured through the satisfaction of the information needs of policymakers (ibid., 92). Intelligence officers also justified bulk collection and refused to acknowledge it as mass surveillance since human eyes are not looking into it due to the large magnitude of data collected daily (Cayford et al. 2018, 98). However, Königs (2002) challenges this evasive perception of mass surveillance by claiming that government surveillance no longer relies on human spies and informers but on technology.

Furthermore, other authors, not merely the intelligence officers, have argued that surveillance and collecting bulk data to solve (security and health) problems is a double-sided delusion (i.e., Flaherty 1986, 9; Andrew 2018; Snowden 2019; McDonald's 2020 in Csernatoni 2020, 303; Lubin 2018). For instance, the historian Christopher Andrew also argues that Intelligence failures often have stemmed from failures to use available intelligence, and that inadequate sharing of information between the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) contributed to the failure to foresee the September 11 terrorist attacks (Foglesong 2019, 964). Hence, making strategic intelligence inefficient for stopping terrorist attacks. Kleining et al. (2011) also explain and exemplify cases of the failure of intelligence collection to prevent catastrophes in the book "Security and Privacy". Also, the case of 9/11, and how the event occurred not due to a lack of intelligence collection, but a general lack of protocols, procedures, and governance managing it, for instance in terms of importance, and scope (Kleining et al. 2011, 127). Lubin (2018) also refutes governments' need to rely on covert (bulk) communications interceptions altogether, perhaps as it has been a demonstratable failure, and as there are fewer intrusive means available to achieve the same "security" aim (530). Similarly, Burt (2019) adds a more technical point of view, by claiming that those who possess enough sensitive personal information, such as companies, governments, or hackers, can pose new dangers to our privacy and security once we generate data. Accordingly, an estimated 2.5 quintillion bytes of data are made daily, and on the rise, making privacy and cyber security issues more pressing over time (Burt 2019, 3) and harder to control. Nevertheless, surveillance and privacy rights should not be undermined, as Bernal (2016) argues that surveillance is power over the individual's personal information, which carries the dangers of blackmail, discrimination, and persuasion (250).

Public health

Within the public health sector, surveillance measures have recently become enforced during the COVID-19 pandemic on a global scope, although accompanied by controversies regarding their effectiveness and overall civil benefits. Authors like Wamsley and Chin-Yee (2021) argue that digital technology in healthcare emerged already in the late 1990s early 2000s, sold as technological fixes to "unprecedented crisis" (2). Similarly, Kitchin (2020) argues that public health is rooted in technological solutionism, best defined as a belief that technology is "the only viable solution to resolve an issue regardless of ancillary costs, and policy is led by technology rather than vice-versa" (373). Alternatively, the standard delusion that more data will solve problems (Flaherty 1986, 9). In addition, others have contested the

effectiveness of these technological mechanisms (e.g., Sekalala et al. (2020), Csernatoni (2020), Kitchin (2020)), contrasting with the WHO's generalized view of surveillance measures as necessary to limit the spread of the virus and resume economic and social activity to the possible extent (Sekalala et al. 2020). Kitchin (2020) combats the generalized belief that during COVID-19 individuals had to choose to renounce their civil liberties for public health forcefully. Particularly addressing several significant issues emerging from surveillance technologies that could be detrimental to democracy and all individuals indistinctively, deeply damaging civil liberties. These dangers include privacy and data leakages, reidentification, population profiling, control creep, erosion of public trust, chilling effects, authoritarianism, Covid washing of activities, and increasing shareholder value and profit (Kitchin 2020, 365). Csernatoni (2020) also addresses "contact-tracing apps" as a "technology theatre" which provides "a form of political cover and spectacle to make people feel safe, but without doing much to "solve" the problem" (Csernatoni 2020, 303). Neglecting the trustworthiness and legitimacy of the entities deploying techno-solutionism, the implications to human rights protection, and if there is enough public understanding of the risks and efficacy of providing sensitive personal data to those technologies (ibid.). Wamsley and Chin-Yee (2021) also argue that digital health technologies exacerbated social and health inequalities serving public interests at the expense of private needs (5). Still, it is uncertain whether these consequences will be prolonged. For instance, Ribeiro-Navarrete et al. (2021) explore rising concerns about the potential misuse of digital surveillance methods during the pandemic by citing Abbas et al., 2020; Calvo et al., 2020; Roth et al., 2020, who stress the potential long-term side effects that may eventually become prejudicial for all individuals (Ribeiro-Navarrete et al. 2021). In essence, enforcing those apps could potentially normalize (surveillance) measures that may modify data privacy and other human rights prospects, leading to the potential rise of new forms of discrimination (Csernatoni 2020, 307-308).

To conclude, this literature review aimed to gather a thorough perspective on the state and relevance of the universal right to privacy. Mass surveillance concerns seem to have drastically changed from the worries of the 1960s to the "I have nothing to hide" ethos of today, possibly perpetuated by the government's generalized use of the "honest citizen" argument. Most notably since the late 1990s alongside the rise of the internet, authors have described how "powerful entities" have abused technology and managed to justify intrusion whilst ignoring privacy rights in exchange for their economic and political interests. Scholars use terms to explain the methods of enhancing surveillance, such as surveillance capitalism, dataism,

personal data as a commodity, or the body as a password. Strikingly, the notion of privacy has not been adequately defined, legally, academically, publicly, or in industries where citizens entrust their data. In academia, scholars have seemingly agreed on a definition of 'control over sharing', although this definition is noticeably limited. The legitimacy and effectiveness in combating security threats of (digital) surveillance have been refuted by both intelligence officers and the literature examined. Although attempts to ban mass surveillance prevail from a legal stance, demonstrated by the "Intelligence Codex" proposal which was rejected, public lack of awareness is possibly the biggest issue when it comes to the success of establishing boundaries to curtail the abuse of personal data. Still, the ongoing interest of policymakers and intelligence in maintaining mass surveillance through security justifications, and ignoring privacy concerns, before its meaning became as simple as control over sharing, has not been formally addressed. Additionally, within the field of public health, surveillance has also been argued to be detrimental to human rights and ineffective, and authors have addressed the potential long-term side effects of the measures implemented during COVID-19. Yet, whether the public health sector, like firms, collaborates in the sharing of information with governments for "policymaking" remains inconclusive.

III. Methods

This chapter explores the methodology for this thesis, which strongly relied on triangulation, a multi-method approach consisting of a cross-case study, analyzed with the critical discourse analysis, process tracing, and explorative research methods, and interpreted through different theories, explained in the theoretical framework. This methodology has several advantages, which include providing a more thorough understanding of this thesis' research problem and increasing the credibility of the findings. One of the limitations of this type of granular research was time-consuming, and more data could always be gathered. Additionally, this chapter presents the type of sources collected, and the research procedure used to formulate and answer the research question, which again is:

How do policymakers increasingly justify policies that erode privacy, and how are these prejudicial to other human rights?

The first steps of the study consisted of exploring the initial topics of interest that this thesis aimed to research, namely, the explanations of mass surveillance and violating privacy rights. For the literature review chapter II, this thesis used secondary qualitative sources, which discussed the perspectives of privacy rights held by different actors, which led to the case studies' selection, and its critical constructivist approach. These sources were found in Google scholar and the Leiden University catalogue and overall served to provide a generalized perspective of privacy by different policymakers, which can constitute individuals from different sectors. One theory reached during this stage was the securitization theory, which is mostly used for case study interpretation, and it is explained in more detail in the theoretical framework section of this chapter. The relevance of the theory of securitization was also encountered by putting the historical background and literature together, and how since the 20th century, surveillance mechanisms have become pervasive and advanced progressively through security concerns. Although convenience is used as a reason to justify the introduction of these systems by Big Tech and enabled by the public views on privacy, as explained in the literature review, security is commonly used by other actors as a reason to justify the erosion of privacy rights.

The cross-case study of these two subjects was also chosen as a method, to test the securitization theory. Also, hypotheses posed by authors like Farrell and Newman in the book "*Of Privacy and Power*", who have argued about the transatlantic struggle over freedom and security, and how different actors abuse globalization to exploit circumstances that enable intrusion. Moreover, according to studies, during substantial and immediate threats, people are prone to embrace surveillance for security (Marciano 2019, 984). Hence, highlighting the political power of 'threats' in advancing surveillance. Chapter IV constitutes a substantial chapter that highlights existing systems in the EU that violate privacy, communications, and biometric surveillance, and justified for security purposes, where their effectiveness and human rights implications are left unquestioned by policymakers. This chapter could contribute to answering the research question, whilst providing first insights into the critique of digital identification systems in IR, or the eID in Europe, that other scholars could further explore.

III.I Cross-Case Study

Given the scope of the research question, the thesis redirected the research to a cross-case analysis, the COVID-19 event and the eID. These cases are explored in Chapter V, and examined through critical discourse analysis, process tracing, and explorative research. The

main sources used for their interpretation were primary and secondary sources. Primary sources like information by a whistleblower found on Google were used to critically examine the securitization of COVID-19 and to provide a different perspective to the one of policymakers. The information from this source was later "fact-checked" or contrasted with other sources found on Google Scholar, and the official websites of the WHO. The WHO and sources from the WEF were also investigated, given the prominent role played by these policymakers during COVID-19. To examine the EU COVID Certificate and the eID, secondary sources such as the official websites of the EU Commission were examined, and primary sources such as reports as well as reports by the WEF, and books by its leader to fuel discussion. First, the discussion deconstructs COVID-19 by using a securitization framework since this was a critical event in the introduction of public health surveillance and the EU COVID Certificate. Here, critical discourse analysis was used to compare the threat declaration by the WHO, the perspectives of the WEF, and a whistle-blower. Process tracing was chosen as a method to explore the link between the EU COVID Pass and the recently launched European Digital Identity (eID). This case is explored since it could exemplify the arguments of the securitization theory of using threats to advance extraordinary measures or the abuse of cross-border threats to advance certain policies as addressed by Farrell and Newman. In this thesis, the demonstration of how COVID-19 (a cross-border threat) is used to advance the eID, potentially through the EU COVID Certificate, is illustrated. However, since this is a novel question, explorative research was used to analyze the link between the eID and the EU COVID certificate, given the lack of existing academic discussion regarding the connection between these two policies. Lastly, critical discourse analysis is also used to address whether the regulations of the eID address the social limitations that the EU COVID Certificate and COVID countermeasures exposed, measured through the human rights framework, or as presented by other scholars.

III.II Theoretical Framework

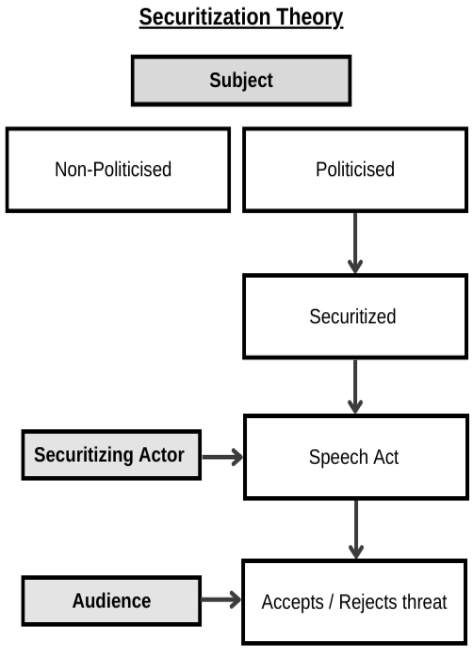
The case study is explored through the Securitisation theory, Agenda-setting and Framing, and Human rights, as described in the UHRD. These theories, due to their underlying critical constructivist approaches, motivated by perspectives encountered in the literature review, were suitable to interpret these cases, whilst formulating an answer to the research question. The *securitization* theory, from the Copenhagen School of Thought, is the theory mostly used in the case study of COVID-19. To give some background, Ole Wæver proposed this theory emerged in the 1980s, as he argued that with the end of the Cold War, the security

agenda widened to include the environmental, economic, societal, and political sectors (Buzan et al. 1998). With the widening of the security agenda in the 1980s, security became a contested subject with no specific definition and directly overlapped with politics. The securitization theory provides a critique of the constructive nature of security dilemmas, which is useful to understand how policymakers used the virus to introduce policies. Security, as defined in the book "Security: A New Framework for Analysis" by Barry Buzan, Ole Wæver, and Jaap de Wilde, is considered "the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics (Buzan et al. 1998, 23)". Securitization can thus be seen as a more extreme version of politicization (ibid). This theory argues that 'security issues' do not exist per se, but they are created by policy actors who frame them as a threat. Through speech acts an issue can be moved into a security frame, achieving extraordinary effects, and justifying extreme measures (Wæver 1993, 22). There are different steps or securitization moves in the securitization theory, used in this thesis to examine COVID-19. First, the "speech act", consists of a discourse presenting something as an existential threat to a referent object (i.e., the War on terror by George W. Bush to American citizens, or a Pandemic declaration by the WHO). And second, "audience acceptance", which determines whether securitization succeeds, as the public must accept the threat as such, for the 'countermeasures' to be legitimate. Nevertheless, audience acceptance can be manipulated, as the literature review argued, using personal information by private companies to change perceptions.

The audience acceptance element in securitization theory is also related to the *agenda-setting and framing theory*, which highlights the role of mediatic content influencing audiences. This theory also overlaps with the experimental agenda of securitization theory, since the media can influence the audience by using extreme terms (i.e., terrorism, pandemic), and repetitive sensorial inducing methods, such as vivid images of the catastrophe, which have a higher degree of public influence (Baele and Thomson 2017, 647). Therefore, the role of the media is essential, since it is a driving factor in the success of securitization and audience acceptance, which consequently leads to accepting the measures due to fearing the ramifications of ignoring the speech act (Buzan et al. 1998, 25). Again, using these Constructivist approaches may help answer the first part of the research question, namely the advances of policies due to the pandemic declaration, whilst advancing a practical understanding of securitization theory. Therefore, shedding light on the problematic nature of securitization, not as a theory, but as a framework in political decision-making, given that threat construction enables actors in

powerful financial positions, to advance private interests. Furthermore, although the main method used throughout this thesis was qualitative research, quantitative data was also used to measure public threat acceptance and to provide figures regarding the financial involvement of different entities during COVID-19. Lastly, the *Human rights* framework is also used extensively in the following chapters to evaluate the social impact or ethical concerns risen by the policies ensuing COVID-19 in the EU, but also on a global scale. This was also used as a parameter to evaluate the repercussions of the eID, where legal human rights considerations are explored.

Figure 1:



IV. Surveillance for Security

This chapter provides a brief additional background on communications and biometrics surveillance, justified as security mechanisms, and their effectiveness. These ongoing forms of surveillance, also present in the EU, are relevant to answer the main research question and to draw conclusions from the human rights considerations of the eID later in Chapter V. II.

IV.I Communications surveillance

The surveillance of digital communications is undergoing through programs like Echelon, which captures all communications data through intercept stations, with the ability to scan for specific words and flag communications. Later, flagged communications are recorded and analyzed (Pfluke 2019, 306). Another comparable program is Pegasus, an Israeli spyware software created by the NSO group that can be installed on iOS and Android, which is currently employed by governments worldwide (Montag et al., 2021). However, the social implications of surveillance mechanisms are concerning. For instance, it has been argued that Pegasus threatens democracy, enables the monitoring of citizens, and is a pathway to dictatorial regimes (Pegg and Kirchgaessner 2021). Yet, strikingly, the NSO Group offered its services and contact tracing solutions during COVID-19 to several governments (Kitchin 2020, 364). Another current risk to privacy is untargeted foreign cyber surveillance, for instance, by non-democratic countries like China, which according to Watt (2017), remains inadequately dealt with (790). In the US, the leaked documents by former NSA member Edward Snowden proved the agency's use of the PRISM and Upstream programs. The latest allows for the "collection of content and communications data from fiber optic cables and infrastructure owned by the US, having access to global data, particularly of non-US citizens" (European Court of Human Rights 2021). The leaks also showed an operation codenamed TEMPORA by the UK Government Communications Headquarters (GCHQ) intelligence services, which enabled it to tap and store huge volumes of data (ibid.).

IV.II Biometric surveillance

Marciano (2019) defines *biometric surveillance* as "the use of automated systems that measure biological (e.g., fingerprint) or behavioral (e.g., gait) characteristics to identify, monitor, and control individuals and populations" (128). Milone (2001) argues that biometric surveillance originated in the Department of Defence program Facial Recognition Technology (FRET) in the US in the early 1990s. Various universities were then selected to work on the 6.5-million-dollar program (501). Supporters considered this type of surveillance as part of their security regime (Milone 2001, 498). Currently, the largest biometric database in the world is in the US Automated Biometric Identification System (IDENT). This system captures the fingerprints of people entering the US, storing more than 130 million records in 2012 (Marciano 2019, 131) and over 200 million in 2021 (Thales 2021). Similarly, in Europe, there

is the EURODAC, a database of the fingerprints of asylum seekers and irregulars crossing the borders (ibid., 131). The European Digital Rights (EDRi) legal analysis of biometric mass surveillance in Europe, sheds light on the rise of facial recognition practices in Europe, and biometric mass surveillance mechanisms in Germany, The Netherlands, and Poland (Montag et al. 2021, 13). Yet, these practices contradict the assumption that people "are safer under systems of biometric mass surveillance", by exemplifying how biometric surveillance tools present in eighteen German cities barely ameliorated crime rates (ibid., 33). Instead, they exacerbate structural discrimination and pose serious threats to people's dignity. Yet, these systems are becoming systematic to the way people exist in Europe, becoming impossible to defend personal biometric information (ibid., 12). Nevertheless, others have also claimed that when done on a large scale and over a long period, digital identification logs can be a tool for pervasive profiling and surveillance (Aggarwal et al. 2018, 17). Additionally, proliferating biometric sensors, such as with the introduction of cameras in public spaces, results in "biometric surveillance" and means of perpetually monitoring the location and behavior of people, eliminating privacy and the right to be left alone (Milone 2001, 497). Also, using biometrics as an authentication mechanism carries significant security risks, namely due to the uniqueness and singularity of biometric information, which would make biometric leaks irreversible (Aggarwal et al. 2018, 16).

V. Cross-Case Study: COVID-19 (2019-2022) and the eID

V.I The Securitization of COVID-19 and Human rights repercussions

This section de-securitizes COVID-19, by analyzing the speech act, its securitization, and the public threat acceptance. This section also explores the actors guiding the response to COVID-19. Then, it challenges the necessity of introducing the measures implemented on a global scale to combat this threat by investigating how these measures violated privacy rights and eroded other human rights. Lastly, it will critically examine how policymakers viewed these measures.

Speech Act

On January 2020, surveillance took a massive shift, with the Public Health Emergency of International Concern (PHEIC) statement, made by Tedros Adhanom, the securitizing actor,

leader of the World Health Organisation (WHO). This was done in the vid of COVID-19, the disease caused by the pathogen SARS-CoV-2 first detected in November 2019, in Wuhan, China (Agostinis et al. 2021, 322), and labeled by the WHO as the COVID-19 pandemic on March 11, 2020 (Murphy 2020, 495). These stages could be considered part of the Speech Act. It could be argued that COVID-19 was a politicized issue. The deathliness of COVID-19 was a subject of considerable dissensus, although citing Klaus Schwab, the leader of the WEF, "COVID-19 has killed less than 0.006% of the world population. To put this low figure into context in terms of lethality, the Spanish flu killed 2.7% of the world's population and HIV/AIDS 0.6%, and the Black Death 30% to 40% of the population" (Schwab and Malleret 2020, 266), or about a third of all Europeans between 1347 and 1351 (ibid., 18). Considering the leader's emphasis on the virus' low lethality, what explains the global response to COVID-19, and the virus' social impact needed to implement the measures used to control the virus?

From the Politicization to the Securitization of COVID-19

The political securitization of viruses like COVID-19 did not emerge immediately with the outbreak of November 2019, but it was disputably, a 2-decade, if not longer, process of political decision-making. Authors like Yee (2021), cited in the literature review, argue that digital technology in healthcare emerged already in the late 1990s early 2000s, sold as technological fixes to "unprecedented crisis" (2). Yet, 2009 was a turning point for the legitimization of COVID countermeasures. Namely, with the WHO changing of the definition of "pandemic" to a contagious rather than contagious and deadly disease, which broadened the scope of alerts or "Emergency declarations" to non-lethal diseases (e.g., Doshi 2011; Singer et al. 2021; Cohen 2009). Moreover, several articles were written in 2003 regarding SARS-Cov, described as a severe acute respiratory syndrome associated with the coronavirus, starting in China, and originating from wild animals (e.g., Drosten et al. 2003). Only, the most recent variant, SARS-Cov 2 was given a Pandemic status. Dr. Stuckelberger, a whistleblower who worked for the WHO on International Health Regulation (IHR) and public emergency management between 2009 and 2013, also claimed that the WHO officially modified the term "herd immunity", into one emphasizing vaccination rather than natural immunity. Yet, this approach to immunity led to several controversies in the scientific community as vaccinations were failing to protect individuals from contracting the virus, providing explanations for this (e.g., Ajana 2021; Robertson 2022). The media and WHO disregarded these reasonings, perhaps as otherwise, the securitization of COVID-19 would have failed as well as the

legitimacy of its countermeasures. Hence, the change in the definition of "pandemic" in 2009 and the change in approach to "herd immunity" served to justify and guide the masses' personal choices, while introducing other surveillance solutions to the pandemic.

The systemic change in the approach to the virus was a turning point in the justification of the measures that states must implement during these PHEIC declarations. According to Dr. Stuckelberger, PHEIC declarations force 196 states to obey the International Health Regulation (IHR) by the WHO "Constitution" with the exceptions of the United States and Iran (Stuckelberger 2022, 10:40). When this was checked on the WHO website, the claims were confirmed, and a booklet called "International Health Regulations" (2005) Third Edition could be downloaded. The IHR is an instrument of international law that is legally binding on 196 countries (World Health Organization n.d.). The European Medicines Agency (EMA) plan for emerging threats from 2018 also supports the claims by Dr. Stuckelberger, by stating the authority of the WHO as well as of the European Commission to declare a PHEIC or a pandemic (EMA 2018, 6). Nevertheless, the measures stated in the IHR were strikingly illiberal and not compliant with human rights standards, even though states listed in the IHR were forced to implement them. Some of these measures included tracing individuals, refusing departure or entry, implementing isolation or quarantine, and placing suspect persons under public health observation (WHO 2016, 17). Moreover, according to the IHR booklet, countries are forced to comply with these measures and periodically report to the WHO, using surveillance and control regardless of the individual's disapproval. In other words, a form of authoritarianism given that civic actions are no longer directly determined by elected leaders.

Public Threat Acceptance: Agenda-setting?

COVID-19 had an undebatable social impact, although arguably more due to its management. When looking up the term "COVID" on google scholar within the time frame of 2000 and 2018, 19.300 results were shown, and only by enlarging the frame 3 years to 2022, 34.800 results popped. According to the New York Times, by November 2022, 71.1% of the world population had received at least one shot to stop COVID-19 (Holder 2022). Moreover, large investments were directed to the pandemic. Only between January 1st, 2020, and June 27, 2020, funding combatting the coronavirus exceeded 21.7 trillion dollars. According to the statistic, 86% of those fundings had an economic link to their objectives, only 1.3% were linked to health goals, and 0.8% were for vaccines and COVID treatment (Cornish 2021).

Agostinis et al. (2021) argue the role of 'Philanthrocapitalism' in advancing private interests during COVID-19, as the Bill and Melissa Gates Foundation (B&MGF) was the second major donor to the WHO (322), and both the B&MGF The Rockefeller Foundation were among the top five donors to the COVID-19 response (323). In addition, Gavi and Bill Gates have repeatedly stressed the need to prepare for upcoming pandemics (e.g., see Gavi n.d., Gates 2022). Remarkably, Dr. Stuckelberger claimed the prominent partnership role of Gavi, a vaccine alliance located in Switzerland, and Bill Gates, who have total legal impunity (Stuckelberger 2022, 7:00; 8:55). Still, according to a study made by the newspaper POLITICO, a sum of 10 billion dollars was directed to the COVID response by only four entities since 2020. These were the Gates Foundation, the Wellcome Trust, the Coalition for Epidemic Preparedness Innovations (CEPI), created in 2017 by Gates and Wellcome Trust, and Gavi, the global vaccine organization that Gates helped to found (Banco et al. 2020). Moreover, Gavi and CEPI, which received considerable funding from the B&MGF together played a critical role in advising governments and the WHO (ibid.). Hence, financially benefiting only a few philanthropists, given their advisory role in vaccine distribution, and ownership of GAVI. Nevertheless, according to the Public Readiness and Emergency Preparedness (PREP) Act of 2005, vaccine manufacturers and qualified persons distributing COVID-19 countermeasures such as Pfizer or Moderna vaccines, are also granted total impunity in emergency declarations from any liability for side effects or deaths (Yin 2020; Sigalos 2020). Surprisingly, in Europe, there is still a lack of transparency regarding the liability of COVID-19 countermeasures, even though countries like Austria made vaccination mandatory in February 2022, with fines for unvaccinated of over 3.600 euros a year (Gomez 2022). Thus, rising critical human rights questions.

Public acceptance of COVID-19 countermeasures could be explained through Agenda-setting and Framing theory, which illuminates the importance of media content in terms of its potential influence on audiences (Marciano 2019). Similarly, private companies can control the masses without people being aware of it or at least changing their habits (Ribeiro-Navarrete et al. 2021, 2). Hence, the media could have also been a predominant method in determining the success of the securitization of COVID-19, given it can influence people's opinions and beliefs, and security perceptions. Already in 1956, the American-Dutch doctor and psychoanalyst Joost Meerloo stressed the importance of freedom of thought as a human right, and the role of media, namely the press, radio, and television, as morale-inducing mediums, like psychological status and behavior (Meerloo 1956, 378). Also, broadcasting the official "truths", and enabling these

to change people's perceptions (ibid., 57). Furthermore, a report by the European Medical Agency (EMA) states that during levels 2 and 3 of the Health Threat Plan, there must be media alerts and increased communication and *message coordination* with institutions outside of the EU, and level 3 emphasizes a more intense mediatic coverage with "ongoing procedures for medical products" (EMA 2018, 6-7). If the COVID-19 pandemic as a high-priority issue lasted from March 2020 until March 2022 approximately, that estimates a period of one year of coordinated and consistent mediatic coverage of the topic, and public pressure to accept the medical product, since half of the levels of the health threat plan focused on increased mediatic coverage. A study conducted in the early stages of the pandemic in Japan on the impact of media channels on mental health during COVID-19 also reported that too much access to media can make people over-amplify the risk of COVID-19, increasing fear and worry about the disease, advising a regulated use of those systems (Sasaki et al. 2020, 502). Sometimes, even exaggerating and providing misinformation about the virus (ibid.). This questions the "official truth" broadcasted by the media and the legitimacy of the justifications used for introducing COVID-19 countermeasures on a global level.

Another remarkable response contributing to Agenda-setting was the introduction of fact-checking agencies on a global scale, like "Newtral". Whereas these agencies were introduced under the justification of combatting 'misinformation', they also served to hide information or evidence and to degrade opinions clashing with the official COVID-19 narrative. For instance, scientists and whistleblowers like Dr. Stuckelberger were depicted in the media as an 'anti-vax', by Newtral and Wikipedia, which consequently led many people to disregard important findings, such as the ones previously mentioned. Again, according to Meerlo (1956), the dismissal opportunity of communicating dissent and opposition as a formula for political conditioning of the masses (57). Given dissidence was coerced due to "mediatic message coordination" established in the Health Plan of the EMA and fact-checking agencies, it could be argued that this response to COVID-19 deeply eroded democracies. Namely, as these inhibited the possibility of freedom of thought and choice, and democratic regimes give the man the dignity to think for himself, have his own opinion, assert it, and protect himself from mental invasion and coercion (ibid., 413). Essentially, people were pressured into choosing a medical option based on ethical motivations dispersed by the media, forcefully having to show their choice through a COVID certificate, and eventually enabling or disabling the individual to participate freely in society. The lack of privacy regarding the person's health status, and freedom of choice, eventually led to discrimination, and the erosion of other

fundamental human rights. This could only be justified in the absence of the knowledge highlighted in this de-securitization of COVID-19.

Human rights repercussions

Overall, justified or not, COVID-19 served to introduce drastic measures that infringed on the right to privacy. Mainly, as these requested a person's health information and were officially used to discriminate against people based on the status shown in their certificate, arguably breaking twelve universal human rights and freedoms, as specified in the footnote, which includes the right to freedom of opinion, freedom of association, and protection against degrading treatment.[1] The countries where these measures were implemented, which followed the orders given by the WHO, confronted the description of authoritarian states since these do not share the liberal values of autonomy and privacy (Kleining et al. 2011). Actors like the WEF openly acknowledged severe human rights violations caused by digital apps introduced during the pandemic. For instance, countries like China, Hong Kong, and South Korea, enforced coercive and intrusive measures of digital tracing, tracking, and controlling individuals' digital actions without consent (Schwab and Malleret 2020, 173). With the launch of applications like "Trace Together," individuals were exposed to unimaginable policy concerns of cyber intrusions, data retention dilemmas, and issues of trust in the system's operator (ibid., 174). Still, despite his awareness of the policy concerns embodied in digital

[1] ***Article 1***: "All human beings are born free and equal in dignity and rights"; ***Article 2:*** *"*Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind (…) or opinion (i.e. vaccine mandate)"*;* ***Article 5****:* *"*No one shall be subjected to torture or to *cruel*, inhuman or *degrading* treatment or punishment"(i.e. France president "I will fuck those unvaccinated" (See e.g. Frenchly 2022)); ***Article 7****:"*entitlement to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination". ***Article 12:*** (…) interference with his privacy, family, and reputation (i.e., COVID vaccination status, leading to social stigmatisation); ***Article 13:*** the right to move freely within a country (i.e., lockdowns, quarantines, travel passes). ***Article 18:*** Freedom of thought, conscience (…) (i.e. news coverage restricted to COVID narrative, no open debate with covid dissidence or scientists (i.e. labels of misinformation), and prohibited to strike (i.e. Canada, (Fung 2022)); ***Article 20****:* "right to freedom of peaceful assembly and association" (i.e. lockdowns); ***Article 21****:* "Everyone has the right to equal access to public service in his country" (i.e. public transport restrictions to non-vaccinated, France); ***Article 22***: "everyone has the right to social security" (i.e. global lockdowns enduring at least for the first 3 months, exacerbating other serious diseases due to lack of medical attention); ***Article 23*****:** "Everyone has the right to work" (i.e. job landings U.S. or Austria targeting non-vaccinated), and the right to form and to join trade unions for the protection of his interests (i.e. , arrests and bank account suspensions of hundreds of mandate dissenters, involved, directly or not, in the truck protests in Canada (Fung 2022)); ***Article 25****:* "everyone has the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control" (i.e. in Spain prohibition to attend funerals of relatives or lack of unemployment security with the cut on unemployment benefits for the unvaccinated in Austria (Kıyağan 2021)) (United Nations General Assembly 1948).

solutions implemented on a global scale during the pandemic, in 2021 the WEF claimed that the pandemic had quickened the need to *identify* and verify the identity of individuals and organizations (World Economic Forum 2021, 8). Moreover, another explanation he provides is that digital interaction has increased unprecedentedly, making trusted, verifiable identity essential (World Economic Forum n.d.). Furthermore, governments on a global scale declared the partial reinstallation of the civil liberties that the pandemic fully erased in its first months, as "the new normality", explained as the digitalization of all human processes (Otaiza 2021), or a new way of understanding public health. Hence, COVID-19 was a justification for techno-solutionism, although policymakers failed to address the effectiveness and social and technological policy failures of COVID-19 digital tracking solutions, and human rights implications of COVID certificates, or the crisis itself.

V.II. The European Digital Identity (eID)

From the EU COVID Certificate to the eID or vice versa?

In Europe, the European Commission introduced the EU Digital COVID Certificate in July 2021, although it was preceded by the discussion of an eID, which was introduced by Vonder Leyen on September 16, 2020 (Von der Leyen 2020). This latest identification system would be available to all Europeans by 2024 with all private information, including university certificates, expenses, health information, websites visited, and identity details such as birth and biometric data (Von der Leyer 2021). Moreover, on March 9th, 2021, also before the EU COVID Certificate was put in motion, the European Commission presented Europe's digital transformation by 2030, where 80% of services would be made digital, and on July 1^{st,} 2021, it launched the EU Digital COVID Certificate. Later, at the "Master of Digital 2022" event, she introduced a budget of 125 billion euros, which she calls a "Marshall Plan" in her discourse, for Europe's digital transformation (Von der Leyer 2022, min 2:10). Here, the president of the Commission emphasized "the need of promoting trust in the European Digital ID, and that it will be beneficial for everyone" (ibid., 5:25; 10:30). However, the interest in accelerating digital identification demonstrated by the WEF and the similarities shared by the EU COVID Certificates and the eID are worth examining, to test whether COVID was abused to advance the introduction of these systems. Main similarities include interoperable systems enhanced with blockchain and their use in a digital ecosystem. The main differences are that the EU COVID Certificate was merely used to show health status regarding COVID-19 whereas the eID integrates public health information and far more detailed personal information, like

banking transactions. The digital infrastructure in which it is built holds strong similarities, and since the EU Covid certificate was held by most Europeans during COVID-19, it could have been a first step toward the introduction of a digital wallet where the eID aims to be set. However, since the eID system is to be implemented by 2024, no actual comparison can be done until then. Yet, the following chart advances this exploration by comparing the traditional ID, the EU COVID certificate, and the eID.

Figure 2:

	Traditional ID	**EU Digital COVID Certificate**	**eID**
Information included	Name, ID number, date of birth, issue date and expire date	Full name, date of birth and COVID Status (vaccine used, date, number of doses or recovery status)	Full name, date of birth, all personal information (health information, university diplomas, biometric data linked to eID…)
Type of document	Physical card	QR Code (digital or paper format) enhanced through blockchain	Dependent on a digital device, which adopts the information in a 'digital wallet' operated through blockchain
Functions	To identify (to prove age, name, or nationality) and to enable free movement within the EU	To access public services in some countries during COVID-19 and to enable free movement during COVID-19 along with a legal identification document (ID, or Passport)	To access public services, like requesting a medical certificate. To open a bank account, present a tax declaration, to identify yourself for a hotel registry, to rent a car by using a digital driving permit, to prove age as a traditional ID card…

The Digital ID as a global policy

Digital Identity systems started to become installed as a global agenda by the World Bank Group (WBG) in 2014, which launched the Identification for Development Initiative (ID4D). The WBG claimed that with over 1 billion people without an official proof of identity this initiative was of extreme urgency, and there was a need for not just introducing normal forms of identities but digital ones (World Bank Group 2018, 2). The WBG re-emphasizes for instance in the 2018 Annual report, that ID systems can be weak, exclusionary, and put people's privacy at risk, justifying the need for improved digital versions (World Bank Group 2018). In February 2017, the WBG released the "Principles on Identification for Sustainable Development: Toward the Digital Age" report, which encompassed ten guiding principles for governments in the implementation of a digital ID (DID) by 2030 on a global scale, following the United Nations Sustainable Development Goals (UNSDGs) (Aggarwal et al. 2018, 5), mainly target 16.9 of offering a legal identity for all. While the WBG has explicitly focused on the development impact of the digital ID, the WEF and the ID2020, which are also involved in the initiative, present other motivations (Burt 2022). They state that these are: GDP growth of 13% by 2030, timesaving 110 billion hours via e-government services, lower fraud costs that could save 1.6 trillion dollars, and the ability to prove and better verify identification in the remote setting that COVID-19 underlined (World Economic Forum n.d.). The B&MGF also showed great commitment to the initiative, by committing 1.27 billion to support global health and development projects (Burt 2022). Also, its contributions to the "ID4D Multi-Donor Trust Fund" of the WBG have been catalytic, according to the WB (The World Bank n.d.). Moreover, already in 2016 at the ID2020 Alliance, a member of Gavi demonstrated great commitment to introducing digital IDs in developing countries to ease "paperwork limitations" (Gruener 2016).

Human rights legal concerns from the eID

Several authors have expressed the deficiencies of digital identification systems by stressing that these systems will only be benefitial to society if they comply with International Human Rights Law, mitigating potential discrimination risks and promoting high privacy and data protection (Beduschi 2019, 4). After exploring the *Aadhaar* in India, the largest digital identification system in the world, Dixon (2017) stressed the need for a "do no harm" mandate,

prioritizing policy over technological development and ensuring privacy and data protection, when implementing digital biometric identity systems (Dixon 2017, 539). In India, the system poses striking weaknesses, as even though it was implemented in 2009 as a voluntary program, its replacement of traditional identification methods has led to issues such as extreme cases of starvation and death. Namely, the Indian government linked the Aadhaar to food rationalizing systems in the country, and biometric failures led many, particularly people from lower casts, unable to access food (Vaid 2021). Yet, this is solely one of the examples occurring with global system replacement, largely unaddressed by digital identification proponents.

In the EU, while the eID's data protection technicalities appear to be covered in the eIDAS regulation, covering subjects like the system's construction through blockchain, there are non-technical questions that are not addressed (European Commission 2022). Mainly, the question of discrimination if the eID replaces traditional forms of identification and it is requested to access public services. For instance, elder citizens lacking digital skills could be affected and marginalized from this transition, or ethnic groups, if the wallet showing their religious information is requested to access a public establishment. Discrimination in the eID is enabled through different legislations, which underline the need for re-considering the concept of security as a political construct, most importantly, after COVID-19. For instance, in 1984, the UN Economic and Social Council developed four principles of circumstances that could be used to infringe on civil and political rights. These conditions were: when applied as a last resort; when prescribed by law; when relating to "*public interests*", and when found necessary, proportional to the *public interest* and without less intrusive or restrictive measures available" (Sekalala et al. 2020). Furthermore, while Europe's General Data Protection Regulation (GDPR) has been praised worldwide as being one of the regulations most concerned with privacy, there are several controversies concerning Article 9 (1). Namely, it states that the collection of biometric data is prohibited unless an exception applies, which makes it lawful for "reasons of *public interest in public health*" like its collection for protecting against 'cross-border threats' (Montag et al. 2021, 50).

However, the reasons for 'public interest' are ambiguous, as these can be easily manipulated as explained in Agenda-Setting and Framing theory. Additionally, Gavi and Bill Gates have repeatedly stressed the need to prepare for upcoming pandemics, which could perpetuate the abuse of the public health justification (e.g., see Gavi n.d., Gates 2022). The leader of the WEF also stated that "the corona crisis is (*so far*) one of the least deadly pandemics

the world has experienced over the last 2000 years" (Schwab and Malleret 2020, 18). His emphasis on "so far" could be explained by the change in the definition of the term pandemic. Rising concerns, since this new definition could be the subject of political abuse if new viruses are given pandemic status, justifying a perpetual mobilization of resources, and redirecting people's decisions through fear of contagion, to adopt certain policies. The WEF also stated that: "In the name of *public health*, elements of personal privacy will be abandoned for the benefit of containing an epidemic (public interest), just as the terrorist attacks of 9/11 triggered greater and permanent security in the name of protecting public safety. Then, without realizing it, we will fall victim to new surveillance powers that will never recede and that could be repurposed as a political means for more sinister ends" (Schwab and Malleret 2020, 180). Since pandemics or global health emergencies enable the GDPR to collect biometric data to stop "cross-border threats" or serve public interests, the eID which intends to be used for all services by 2030, creates the ideal system of political control, shattering western democracies and summing to the argument by Marciano (2018) on the technocratization of citizenship (129). Hence, the parallel existence of the eID with ongoing and progressive forms of communications and biometrics surveillance (discussed in chapter IV.II), would enable a landscape of legal control and discrimination of citizens based on their private information, eradicating human rights.

VI. Conclusion

This thesis aimed to answer the question of: *How do policymakers increasingly justify policies that erode privacy, and how are these prejudicial to other human rights?* by taking a securitization approach to the cross-case-study research of COVID-19 and the digital identity in Europe (eID). One evident answer to this question is security. Historically and presently, security has been used, if not abused, by policymakers to advance policies that invade people's privacy. Communications surveillance began with the Five Eyes Alliance to stop a security concern, which was Communism during the Soviet Union, but governments still use Echelon, and the Alliance has expanded. Biometric surveillance entered into force with 9/11, although the funding of these systems began before, and in Europe, it is increasingly being enforced in public spaces with facial recognition cameras. The cross-case study examination of COVID-19 and the introduction of the eID, through securitization also validated the politics of

surveillance hypothesis by Farrell and Newman. Currently, the GDPR enables the collection of biometric data to serve public interests or combat cross-border threats although this form of the legal grey area has not been critically examined. The change in the terms of pandemic and herd immunity also enlarges the possibilities of abusing this justification. Overall, human rights violations, including privacy rights violations, must never be accepted as these could lead to historical repetition and fatalities such as the ones leading to the foundation of the UHRD in 1948. Thus, the developments that endanger these rights must be cautiously re-examined. If unresolved, these dilemmas could pose serious human rights issues, as well as legitimacy and accountability questions that could affect global governance.

As of the contributions made by this thesis, within the field of IR, scholars like Marion et al. (2021) have acknowledged that the role of philanthropy has been vastly unrecognized. The cross-case study of COVID-19 and the eID addressed this gap, as these highlighted a critical finding, which was the decision-making role of philanthropy in both cases. Most notably, of the B&MGF, Gavi, and other elite actors pushing digital identification policies, like the WEF, the ID2020, and the WBG, where the B&MGF also plays a huge financial role. This thesis' critical constructivist approach used to interpret the COVID pandemic and the progression of Digital identification systems, challenged the legitimacy of their decisions, and the need for techno-solutionism. The eID or the regional adoption of digital identification in Europe by 2030, was already underlined in many documents before the pandemic, which includes the WBG guideline launched in 2017 "Principles on Identification for Sustainable Development: Toward the Digital Age", UNSDG 16.9 "Digital Identification for all by 2030", or the ID2020 initiative launched in 2016. The pandemic, arguably accelerated its adoption, posing privacy concerns after examining the potential manipulative role of the media, predisposing the meaning of "public interests" or "threats". One evident shortcoming of the eID, which is highlighted in this thesis, is that it could be used as a discriminatory and control mechanism, as it occurred with COVID certificates during the pandemic. These issues are up until this day dismissed and constitute a critical public policy concern in the launch of the eID. Highlighting, the relevance of privacy during COVID-19, as threats can be abused and governments can change regulations, requesting certain personal information to access public services such as vaccination. This finding also underlines the need to reconsider the meaning of security. The solution to the pandemic was an example, with policymakers' legal lack of liability in the medical solution they proposed, through the PREP Act.

This thesis also underlined the limitations of the definition of privacy, which in academia has turned into one emphasizing "control over sharing". This approach to privacy is outlined in the eID policy, and the use of 'blockchain', which limits the possibility of personal data being collected by third parties. More specifically, as the president of the European Commission stated that this wallet would enable citizens to control all their generated data, which is threatened and insecure every time a citizen logs into a website. Although this would solve the cyber-security data leakages of contact-tracing apps, her speech or the eIDAS regulation did not regard discrimination issues, which were a critical question during COVID-19. Discrimination or technical failure dilemmas are also ignored in countries where digital identifications are enforced, as these are portrayed as role models. Therefore, this thesis challenged the "control over sharing" definition of privacy, by emphasizing the need for one more alike to the principles of Article 12 of the UHRD, which again states that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to legal protection against such interference or attacks" (United Nations General Assembly 1948).

An alternative approach to privacy would legally disable the request of personal information to access public services, including health or vaccination status, and the attacks on the individual's reputation, through job contract terminations based on this information, which occurred during COVID-19. Therefore, without policymaker's reconsideration of privacy, a "do no harm", and a re-examination of critical contestations of the COVID-19 crisis by officials, the long-term benefits of the eID may only be defined by the interests met by its proponents. Re-stating Flaherty (1986), the way privacy protection debates are solved today will have far greater implications for the future. Still, the normalcy in which privacy violations occurred during COVID-19 remains distressing.

One evident limitation of this research resided in aiming to examine the term "justification" used in the research question, as it was difficult to define or find precise answers to this question. Hence, this thesis delved into theories that simultaneously challenged these justifications while pinpointing them. Although, justifications could perhaps only be found through direct interviews with policymakers. For instance, by asking them critical questions regarding the legitimacy of COVID-19 in the implementation of COVID Certificates and their

technical similitude with digital identification ideals. Yet, this is an impossibility, considering the financial and time resources of this research. Also, they would possibly smile and say, “there is nothing you should worry about” as intelligence officers according to Lubin (2018), leading to a less critical answer. Another limitation was examining an event fueled with controversies in a sensitive way, which arises from de-securitization. Yet, presenting these controversies was critical to challenge policymaker’s COVID-19 countermeasures and their unaddressed implications. Also, to highlight the malleability of terms like public interests or public health referred to as the perversion of language by the influential novelist George Orwell. The third limitation was choosing a case that has not been implemented yet, the eID. Nevertheless, this was both a limitation and a contribution, considering it could open further debate before the policy is implemented with no alternative but adoption, as it occurred in countries where digital identification was initially launched as voluntary. Overall, trust in these systems, as requested by the president of the European Commission, may only be achieved once these debates are adequately dealt with. Until then, the trustworthiness of the eID as an instrument prospectively replacing traditional identification systems can be subjected to human rights concerns.

References

"Case of Big Brother Watch and Others v. The United Kingdom.," European Court of Human Rights (Grand Chamber 2021). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}.

"EMA Plan for Emerging Health Threats." European Medicines Agency, December 10, 2018. https://www.ema.europa.eu/en/documents/other/ema-plan-emerging-health-threats_en.pdf.

"Trudeau vows to freeze anti-mandate protesters' bank accounts." *BBC* (News US & Canada), February 15, 2022. https://www.bbc.com/news/world-us-canada-60383385.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2 (June 1, 2016): 442–92. https://doi.org/10.1257/jel.54.2.442.

Aggarwal, Naman M., Wafa Ben-Hassine, and Raman Jit Singh Chima. "National Digital Identity Programmes: What's next?" Published March 21, 2018. https://www.accessnow.org/national-digital-identity-programmes-whats-next/.

Agostinis, Giovanni, Karen A Grépin, Adam Kamradt-Scott, Kelley Lee, Summer Marion, Catherine Z Worsnop, Ioannis Papagaryfallou, et al. "FORUM: COVID-19 and IR Scholarship: One Profession, Many Voices." *International Studies Review* 23, no. 2 (May 23, 2021): 302–45. https://doi.org/10.1093/isr/viab004.

Ajana, Btihaj. "Immunitarianism: Defence and Sacrifice in the Politics of Covid-19." *History and Philosophy of the Life Sciences* 43, no. 1 (March 2021): 25. https://doi.org/10.1007/s40656-021-00384-9.

Amnesty International UK. "Why Edward Snowden Should Be Pardoned," October 19, 2020. https://www.amnesty.org.uk/edward-snowden-nsa-whistleblower-pardon.

Andrew, Christopher M. *The Secret World: A History of Intelligence*. The Henry L. Stimson Lectures Series. New Haven: Yale University Press, 2018.

Baele, Stéphane J., and Catarina P. Thomson. "An Experimental Agenda for Securitization Theory." *International Studies Review* 19, no. 4 (December 1, 2017): 646–66. https://doi.org/10.1093/isr/vix014.

Banco, Erin, Ashleigh Furlong, and Lennart Pfahler. "How Bill Gates and partners used their clout to control the global Covid response — with little oversight." *Politico,* September 14, 2022.

https://www.politico.com/news/2022/09/14/global-covid-pandemic-response-bill-gates-partners-00053969.

Beduschi, Ana. “Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights.” *Big Data & Society* 6, no. 2 (July 2019): 205395171985509. https://doi.org/10.1177/2053951719855091.

Bennett, Colin J., and Charles D. Raab. “Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective.” *Regulation & Governance* 14, no. 3 (July 2020): 447–64. https://doi.org/10.1111/rego.12222.

Bernal, Paul. “Data Gathering, Surveillance, and Human Rights: Recasting the Debate.” *Journal of Cyber Policy* 1, no. 2 (July 2, 2016): 243–64. https://doi.org/10.1080/23738871.2016.1228990.

Burt, Andrew. “Privacy and Cybersecurity Are Converging. Here’s Why That Matters for People and for Companies.” *Harvard Business Review*, January 3, 2019. Cybersecurity And Digital Privacy. https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies.

Burt, Chris. “Gates Foundation commits $200M to digital ID and other public infrastructure.” *Biometric Update*, September 27, 2022. https://www.biometricupdate.com/202209/gates-foundation-commits-200m-to-digital-id-and-other-public-infrastructure.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 1998.

Cayford, Michelle, and Wolter Pieters. “The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying.” *The Information Society* 34, no. 2 (March 15, 2018): 88–103. https://doi.org/10.1080/01972243.2017.1414721.

Cohen, Elizabeth. “When a pandemic isn’t a pandemic.” *CNN*, May 4, 2009. https://edition.cnn.com/2009/HEALTH/05/04/swine.flu.pandemic/index.html.

Cornish, Lisa. “Interactive: Who’s funding the COVID-19 response and what are the priorities?” *Devex*, July 21, 2021. https://www.devex.com/news/interactive-who-s-funding-the-covid-19-response-and-what-are-the-priorities-96833.

Csernatoni, Raluca. “New States of Emergency: Normalizing Techno-Surveillance in the Time of COVID-19.” *Global Affairs* 6, no. 3 (May 26, 2020): 301–10. https://doi.org/10.1080/23340460.2020.1825108.

Dixon, Pam. “A Failure to ‘Do No Harm’ -- India’s Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.” *Health and Technology* 7, no. 4 (December 2017): 539–67. https://doi.org/10.1007/s12553-017-0202-6.

Doshi, Peter. “The Elusive Definition of Pandemic Influenza.” *Bulletin of the World Health Organization* 89, no. 7 (July 1, 2011): 532–38. https://doi.org/10.2471/BLT.11.086173.

Drosten, Christian, Stephan Günther, Wolfgang Preiser, Sylvie van der Werf, Hans-Reinhard Brodt, Stephan Becker, Holger Rabenau, et al. “Identification of a Novel Coronavirus in Patients with Severe Acute Respiratory Syndrome.” *New England Journal of Medicine* 348, no. 20 (May 15, 2003): 1967–76. https://doi.org/10.1056/NEJMoa030747.

European Commission. “The Digital Decade of Europe: digital goals for 2030.” Accessed January 30, 2023. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es.

European Commission. “Shaping Europe’s digital future: eIDAS Regulation.” Updated June 7, 2022. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

Farrell, Henry, and Abraham L. Newman. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton University Press, 2019. https://doi.org/10.2307/j.ctvc77d1f.

Flaherty, David H. “Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies.” *Science, Technology, & Human Values* 11, no. 1 (1986): 7–18.

Foglesong, David S. “From Moses to Edward Snowden: Toward a Global History of Intelligence.” *Diplomatic History* 43, no. 5 (November 1, 2019): 963–67. https://doi.org/10.1093/dh/dhz031.

Frenchley. “Did President Macron Take a Shit on France’s Unvaxxed?” Last modified January 6, 2022. https://frenchly.us/did-president-macron-take-a-shit-on-frances-unvaxxed/.

Fung, Katherine. “Banks Have Begun Freezing Accounts Linked to Trucker Protest.” *Newsweek* Published February 18, 2022. https://www.newsweek.com/banks-have-begun-freezing-accounts-linked-trucker-protest-1680649.

Galantonu, Dumitrina. “The Big Brother Fear.” *American Intelligence Journal* 33, no. 1 (2016): 59–64.

Gates, Bill. *How to prevent the next pandemic*. Google Books, May 19, 2022.

Gavi. “Next Pandemic.” Vaccines work. Accessed November 23, 2022. https://www.gavi.org/vaccineswork/tag/next-pandemic.

Gomez, Julian. “The backlash against Austria's mandatory COVID-19 vaccine law.” *Euronews*, March 9, 2022. https://www.euronews.com/2022/03/04/the-backlash-against-austria-s-mandatory-covid-19-vaccine-law.

Gruener, Dakota. “In a digital world, there's no excuse for more than a billion people to lack an official identity”. World Economic Forum. Last modified December 2, 2016.

https://www.weforum.org/agenda/2016/12/in-a-digital-world-theres-no-excuse-for-more-than-a-billion-people-to-lack-an-official-identity.

Holder, Josh. "Tracking Coronavirus Vaccines around the World." *The New York Times*, November 21, 2022. https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html.

Kıyağan, Aşkın. "Austria to cut unemployment pay to those who refuse COVID vaccine," *AA*, September 17, 2021. https://www.aa.com.tr/en/europe/austria-to-cut-unemployment-pay-to-those-who-refuse-covid-vaccine/2366946.

Königs, Peter. "Government Surveillance, Privacy, and Legitimacy." *Philosophy & Technology* 35, no. 1 (March 2022): 8. https://doi.org/10.1007/s13347-022-00503-9.

Mansfield-Devine, Steve. "Monitoring Communications: The False Positive Problem." Computer Fraud & Security 2013, no. 9 (September 2013): 5–11. https://doi.org/10.1016/S1361-3723(13)70079-4.

Marciano, Avi. "Reframing Biometric Surveillance: From a Means of Inspection to a Form of Control." *Ethics and Information Technology* 21, no. 2 (June 2019): 127–36. https://doi.org/10.1007/s10676-018-9493-1.

Marciano, Avi. "The Discursive Construction of Biometric Surveillance in the Israeli Press: Nationality, Citizenship, and Democracy." *Journalism Studies* 20, no. 7 (May 19, 2019): 972–90. https://doi.org/10.1080/1461670X.2018.1468723.

McDonald, Matt. "Securitization and the Construction of Security." *European Journal of International Relations* 14, no. 4 (December 2008): 563–87. https://doi.org/10.1177/1354066108097553.

Meerloo, Joost Abraham Maurits. *The Rape of the Mind : The Psychology of Thought Control, Menticide, and Brainwashing*. Cleveland: ProgressivePress.com, 1956.

Milone, MG. "Biometric Surveillance: Searching for Identity." *The Business Lawyer* 57, no. 1 (2001): 497–512.

Murphy, Michael P. A. "COVID-19 and Emergency ELearning: Consequences of the Securitization of Higher Education for Post-Pandemic Pedagogy." *Contemporary Security Policy* 41, no. 3 (July 2, 2020): 492–505. https://doi.org/10.1080/13523260.2020.1761749.

NSA. "Signals Intelligence (SIGINT) Overview." Accessed November 14, 2022. https://www.nsa.gov/Signals-Intelligence/Overview/.

Otaiza, Ricardo Gil. "Detrás De La Nueva Normalidad. Behind the New Normality." *Revista GICOS* 6, no. 3 Especial 2 (2021).

Pegg, David, and Stephanie Kirchgaessner. “Pegasus: the spyware technology that threatens democracy.” The Guardian. Published on July 19, 2021. YouTube video. https://youtu.be/G7H9uo3j5FQ.

Pfluke, Corey. “A History of the Five Eyes Alliance: Possibility for Reform and Additions: A History of the Five Eyes Alliance: Possibility for Reform and Additions.” *Comparative Strategy* 38, no. 4 (July 4, 2019): 302–15. https://doi.org/10.1080/01495933.2019.1633186.

Robertson, David. “How we got herd immunity wrong.” *Stat*, March 25, 2022. https://www.statnews.com/2022/03/25/how-we-got-herd-immunity-wrong/.

Rusinova, Vera. “Privacy and the Legalisation of Mass Surveillance: In Search of a Second Wind for International Human Rights Law.” *The International Journal of Human Rights* (August 2021): 1–17. https://doi.org/10.1080/13642987.2021.1961754.

Sasaki, Natsu, Reiko Kuroda, Kanami Tsuno, and Norito Kawakami. “Exposure to Media and Fear and Worry about COVID -19.” *Psychiatry and Clinical Neurosciences* 74, no. 9 (September 2020): 501–2. https://doi.org/10.1111/pcn.13095.

Schwab, Klaus, and Thierry Malleret. *Covid-19 the great reset*. Edition 1.0. Cologne/Geneva: Forum Publishing, 2020.

Schwab, Klaus. *The Fourth Industrial Revolution*. First U.S. edition. New York : Crown Business, 2016.

Sigalos, MacKenzie. “You can’t sue Pfizer or Moderna if you have severe Covid vaccine side effects. The government likely won’t compensate you for damages either.” *CNBC*, December 17, 2020. https://www.cnbc.com/2020/12/16/covid-vaccine-side-effects-compensation-lawsuit.html.

Singer, Benjamin J., Robin N. Thompson, and Michael B. Bonsall. “The Effect of the Definition of ‘Pandemic’ on Quantitative Assessments of Infectious Disease Outbreak Risk.” *Scientific Reports* 11, no. 1 (January 28, 2021): 2547. https://doi.org/10.1038/s41598-021-81814-3.

Snowden, Edward J. *Permanent Record*, 2019. https://www.overdrive.com/search?q=A81DC622-619D-4587-9765-7E8D7F8D76CD.

Stokel-Walker, Chris. “COVID Restrictions Are Lifting — What Scientists Think.” *Nature* 603, no. 7902 (March 24, 2022): 563–563. https://doi.org/10.1038/d41586-022-00620-7.

Stuckelberger, Astrid. “Dr. Reiner Fuellmich with WHO Whistleblower Dr. Astrid Stuckelberger on Gates and GAVI.” *ClearNFO*, February 14, 2022. https://www.bitchute.com/video/vhQv2ij5tjZE/.

Thales. “DHS’s Automated Biometric Identification System IDENT – the heart of biometric visitor identification in the USA.” Published January 19, 2021.

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system.

The World Bank. "Initiative of the World Bank Group." ID4D, accessed November 15, 2022. https://id4d.worldbank.org/who-is-involved.

United Nations General Assembly. *Universal Declaration of Human Rights.* Paris: 1948. Accessed November 18, 2022. http://www.un.org/en/universal-declaration-human-rights/.

Vaid, Dharvi. "The link between India's biometric ID scheme and starvation." *New Delhi,* March 26, 2021. https://www.dw.com/en/the-link-between-indias-biometric-identity-scheme-and-starvation/a-57020334.

Von der Leyer, Ursula. "European Digital identity - Message by President von der Leyen." European Commission. Posted on June 2, 2021. YouTube Short. https://youtube.com/shorts/EFIs-oL1c4g?feature=share.

Von der Leyer, Ursula. "European Digital Identity." European Commission. Communicated on September 16, 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en#why-is-it-needed.

Von der Leyer, Ursula. "Keynote speech by President von der Leyen at the 'Masters of Digital 2022' event." European Commission, Brussels, February 3, 2022. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_746.

Wamsley, Dillon, and Benjamin Chin-Yee. "COVID-19, Digital Health Technology and the Politics of the Unprecedented." *Big Data & Society* 8, no. 1 (January 2021): 205395172110194. https://doi.org/10.1177/20539517211019441.

Watt, Eliza. "'The Right to Privacy and the Future of Mass Surveillance.'" *The International Journal of Human Rights* 21, no. 7 (September 2, 2017): 773–99. https://doi.org/10.1080/13642987.2017.1298091.

World Bank Group. *Identification for Development ID4D 2018 Annual Report.* ID4D. December 31, 2018.

World Economic Forum. "Digital Identity Ecosystems: Unlocking New Value an Interactive guide for executives." September 2021. Accessed June 2022. https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf.

World Economic Forum. "Digital Identity: The Economic Value of Digital Identity." Strategic Intelligence. Accessed November 24, 2022. https://intelligence.weforum.org/topics/a1G0X000005JJGcUAO/key-issues/a1G0X000006NuoVUAS.

World Economic Forum. *The Global Risks Report 2021 Insight Report*. 16th ed. Geneva (Switzerland): 2021.

World Health Organization. *International Health Regulations (2005)*. 3rd ed. Geneva: World Health Organization, 2016. https://apps.who.int/iris/handle/10665/246107.

Yin, Eva F. "Basics of the PREP Act and Liability Immunity for COVID-19 Countermeasures." Wilson Sonsini. July 13, 2020. https://www.wsgr.com/en/insights/basics-of-the-prep-act-and-liability-immunity-for-covid-19-countermeasures.html.