Government, Technology, and Crisis: Balancing Surveillance Benefits and Privacy in Dealing with the COVID-19 Pandemic

Jonas Lund-Tønnesen

PhD Thesis

Department of Political Science

Faculty of Social Sciences

University of Oslo

December 2023

Series of dissertations submitted to the
Faculty of Social Sciences, University of Oslo
No. 1009

ISSN 1504-3991

Cover: UiO.
Print production: Graphic center, University of Oslo.

Abstract

In the modern, digital society, governments, regulatory agencies, and citizens must often make difficult assessments about the benefits of surveillance against the preservation of privacy – a highly regarded value by many. This trade-off is exacerbated in times of crisis, as under these conditions uncertainty reigns, core values of society are threatened, and urgent decision-making is crucial. This is largely underexplored territory in the field of public administration and crisis management. To fill this gap, this thesis addresses the following overarching research question: *How do governments, regulatory agencies, and citizens balance surveillance benefits against privacy in times of crisis?*

The thesis answers this question by focusing on how governments use digital surveillance technology in crisis management, as well as how that technology is legitimized and regulated. Additionally, it investigates the effect of a major crisis on citizens' attitudes toward government surveillance and privacy. These issues are explored in the COVID-19 pandemic using qualitative and quantitative data. The data includes 51 interviews with political and administrative elites as well as regulatory actors and regulatees in Norway, a range of documents from Germany, Norway, and the United Kingdom, and survey experimental data with 23,912 individuals across 16 European countries.

The main findings of the thesis are that governments, regulatory agencies, and citizens make rather different assessments about surveillance benefits and privacy in times of crisis, for many reasons. Governments focus on the benefits of digital surveillance technology in the crisis management system and assess them against other crisis measures, as well as the potential of surveillance to increase governance capacity and governance legitimacy. In regulating the same technology, regulatory agencies devote their attention to the proportionality of surveillance intrusion towards protecting public health and privacy, and base their interventional approaches on intra-crisis experience, the response of regulatees, and levels of urgency and uncertainty. To better explain these regulatory interventions and the assessments made by regulatory agencies in crises, I developed an analytical framework that differentiates between rule-based, norm-based, and idea-based regulatory interventions. This framework expands our understanding of the regulation of emerging technology to crisis situations.

Empirically, the focus is on contact tracing technologies developed during the pandemic to support governments' crisis management. In Norway, as in many other countries, this technology was controversial. The government ended up with an ineffective technology, which weakened crisis management capabilities but retained privacy. The same type of technology is the basis for comparing legitimacy strategies in Germany, Norway, and the United Kingdom. The thesis finds that the countries differ in their emphasis on pragmatic, moral, and cognitive aspects in their legitimacy strategies. A key reason for this is that countries have different historical practices with regards to surveillance and privacy.

Moreover, analyzing survey experimental data in 16 countries, I find that a major crisis such as a pandemic makes citizens more accepting of government surveillance, compared with a non-pandemic setting. This effect is moderated by different types of trust: political trust,

social trust, and trust in the government's capacity to handle the pandemic. For the two latter types, trust matters more for acceptance of surveillance in a pandemic than in a non-pandemic setting. Thus, the thesis contributes to the literature by providing causal explanations about influences on attitudes towards government surveillance and by advancing our knowledge of trust in connection with surveillance and major crises.

Overall, the findings of this thesis provide novel insight and contribute to our understanding of how different actors balance surveillance benefits and privacy in modern times infused with crisis, surveillance, and technology.

Acknowledgements

Many individuals and organizations have contributed to making this thesis possible. I would like to sincerely thank my main supervisor Tobias Bach, who, in my opinion, is an exemplary scholar. Your guidance, encouragement, and commitment to high-quality research made the writing and completion of this thesis much easier. Even with a busy schedule, your physical and digital door was always open to provide insightful feedback and give me something to think about, and I very much appreciate that.

I would also like to express heartfelt thanks to my second supervisor, Lise Rykkja. Thank you for introducing me to academia, continually supporting and encouraging me, and for your professional feedback and advice over many years.

Additionally, I would like to thank my co-author Tom Christensen for an enjoyable collaboration (also beyond this thesis), and for feedback and discussions on many parts of this thesis. Thanks also to my wonderful friend and co-author Christer Flatøy, for all mountain hikes and long conversations over the years. I also want to thank Jostein Askim and Martin Lodge for thoroughly reading and commenting on all parts of the thesis.

Doing a PhD in a department such as the Department of Political Science at the University of Oslo is a fantastic opportunity and an adventure, and I have benefited from intellectual and non-intellectual conversations with many people. The research and teaching environment of the PBO/OPA groups has been especially significant to me, and I want to thank Elin Boasson, Jens Jungblut, Jan Erling Klausen, Kristoffer Kolltveit, Yves Steinebach, Signy Vabo, and all other members.

Moreover, I would particularly like to highlight appreciation for insightful and valuable feedback, comments, and support from Andrew Bennett, Morten Egeberg, Julia Fleischer, Staffan Kumlin, Per Lægreid, and Charles Raab, as well as all participants at various seminars and conferences I have attended including EGPA, ECPR, the national political science conferences, and the Geilo seminars. Thanks also to Lukas and Camilla at the University of Potsdam for hosting me during my stay.

As a PhD candidate, one is not alone, and the journey is shared with many others. A special thanks to Karin, Anna, Ari, Magnus, Erlend, Leif, Lise, Mo, Tamta, Sverke, Betina, Bjørn, and all other internal and external PhD candidates during my time at the department. Furthermore, thanks to all students that I have met and taught, and who (probably unknowingly) have also educated me in many ways. Thanks as well to the administrative staff at the department and the faculty, as well as the cleaning staff for all technical assistance.

I would like to thank all my friends and my family, especially my mother Inger, and my father Jan, for support and love throughout my life.

Lastly, and most importantly, I would like to thank Helene. I am eternally grateful for your presence in my life and for your unconditional love. Your unwavering belief in me through the highs and lows of life makes it far more meaningful.

Jonas Lund-Tønnesen

December 2023

Table of Contents

Part I:
Introduction

1. Introduction

On March 11, 2020, the outbreak of the coronavirus (COVID-19) was declared a global pandemic by the World Health Organization (Cucinotta and Vanelli, 2020). A pandemic is a situation involving deep uncertainty, with threats to human lives and core functions in social systems all across the world (Ansell et al., 2010; Morens and Taubenberger, 2011). In dealing with the COVID-19 pandemic, war-like rhetoric was frequently used by governments to describe the situation, and it was stressed that there was a need to "fight" the crisis in order to get back to "normality" (Boersma et al., 2022, p. 3). This "fight" extensively involved surveillance-related initiatives that instantly affected citizens' personal lives, mobility, social contacts, and working conditions (Vargo et al., 2021; Boersma et al., 2022). Crises such as a pandemic can create windows of opportunity for governments to expand their surveillance through framing the situation as war-like and by employing measures such as digital surveillance technology.

However, such initiatives are often controversial. On the one hand, surveillance can provide vital information and an overview of a situation, and give a sense of control, safety, and security (Cayford and Pieters, 2018). This surveillance-based information can contribute to improving the effectiveness of decision-making and crisis management systems (Kamel Boulos et al., 2011). On the other hand, there are numerous warnings from culture and literature such as George Orwell's dystopian novel *Nineteen Eighty-Four*, about not being too naïve regarding the optimistic promises of surveillance (Richards, 2012). From this perspective, it is argued that surveillance can violate individuals' privacy and personhood, and their exercise of basic rights and freedoms (Whitman, 2004; Richards, 2021). These competing perspectives create difficult assessments for governments, regulatory agencies, and citizens in managing the desire for control, safety, and security, and improving governmental crisis management systems through surveillance, while simultaneously maintaining privacy – regarded as an important value in many societies. Particularly in times of crisis, as in the COVID-19 pandemic, the challenges of finding an appropriate balance between these values and perspectives are intensified and deepened when the crisis persists, and problems and demands change over time under great uncertainty (Boin et al., 2020).

The struggle of balancing competing values and perspectives of this kind relates to longstanding discussions in political science. Prominent thinkers such as Aristotle, Mill (1859), and Weber (1922) have thoroughly explored the issue of the prospect and limits of the control and interference governments can exercise over individual citizens. With both crises

(Tierney, 2014) and surveillance (Lyon, 2015) having become integral components of modern societies, this issue now presents itself under new circumstances. Fundamental to the tensions between government inference and the maintenance of privacy rights for citizens in these circumstances are digital technologies. Whereas research on digital technologies and their surveillance and privacy implications is extensive (Lyon, 2007; Bélanger and Crossler, 2011; Smith et al., 2011; Degli Esposti et al., 2021), research on digital technologies related to crisis and crisis management with a point of departure from public administration is scarce (Boersma and Fonio, 2018). Studies in this and adjacent fields have been more concerned with (digital) technology as a problematic issue that must be dealt with, rather than as part of the system and as a means in crisis management (Perrow, 1984; Beck, 1992; Evan and Manion, 2002; Boin et al., 2005; Boin and Lodge, 2016). Now that digital technology is part of the toolbox for handling crises such as the COVID-19 pandemic (Boersma et al., 2022), it must be understood accordingly. In other words, if we are to properly interpret the relationship between governments and citizens in the contemporary and future world encompassing crisis and surveillance, we need to understand the manner in which digital surveillance technology is utilized, regulated, and legitimized by government in crisis circumstances, as well as how citizens respond to governments' approaches towards using surveillance measures. Therefore, this thesis addresses the following overarching research question:

How do governments, regulatory agencies, and citizens balance surveillance benefits against privacy in times of crisis?

Dealing with conflicting perspectives, goals, and values of this kind is often viewed as a matter of "balancing", i.e., striking trade-offs among competing demands and values of involved actors (Thacher and Rein, 2004; Head and Alford, 2015). I do not take the point of departure that an optimal balance is commensurable as in a rational cost-benefit analysis (Oldenhof et al., 2014), but instead seek to capture which assessments and responses are made under crisis conditions by these actors and explain why they chose a specific course of action. Accordingly, the following sub-questions are formulated:

1. *How do governments use digital surveillance technology in crisis management?*
2. *How is digital surveillance technology legitimized and regulated in times of crisis?*
3. *Does a major crisis affect citizens' attitudes towards government surveillance and privacy?*

These questions are addressed through four research articles, all of which focus on the COVID-19 pandemic. Table 1 provides an overview of the articles. All four articles contribute to answering the overarching research question and in their own way address surveillance and privacy in crisis and crisis management. They are differentiated by the focus on different actors and different processes. **Article 1** concentrates on regulation, and therefore has a primary focus on sub-question 2. **Article 2** and **Article 3** are concerned with governmental crisis management and sub-question 1 but also attend to the legitimacy aspects in sub-question 2. Additionally, **Article 2** includes governance capacity and **Article 3** pays attention to institutional privacy regimes and legacies. Articles 1, 2, and 3 have a specific digital surveillance technology at their center of interest, namely contact-tracing applications. **Article 4** has sub-question 3 at its core and focuses on citizens' attitudes towards surveillance and privacy more generally.

Table 1. Overview of the studied phenomena and the specific sub-questions in the articles.

	Article 1	**Article 2**	**Article 3**	**Article 4**
Phenomena studied	Regulation of emerging technology in crisis	Dynamics of governance capacity and legitimacy in crisis management	Strategic legitimizing of digital surveillance technology in crisis management	Causal effect of a pandemic and associations of trust on attitudes towards government surveillance and privacy
Research questions	Which interventions do regulators use to regulate emerging technology in times of crisis? What are the conditions under which regulators adapt their choice of interventions for emerging technologies in crisis?	What characterized the two processes of developing digital contact-tracing technology in Norway during the COVID-19 pandemic with regards to the dynamics of governance capacity and legitimacy? How can we understand the use of the contact-tracing technology in relation to the other measures to deal with the pandemic?	How did governments in Germany, Norway, and the United Kingdom legitimize their contact tracing applications in the COVID-19 pandemic? To what extent are these approaches in line with privacy regimes and overall crisis strategies in the three countries? How can path dependency explain the adopted legitimacy strategies?	How does a pandemic setting affect individuals' attitudes towards government monitoring of the public? Do various forms of trust matter more for individuals' attitudes towards government monitoring of the public in a pandemic setting than in a general, non-pandemic setting?

1.1 Contributions

The study makes empirical and theoretical contributions to the literature on public administration, crisis management, and surveillance. Empirically, it provides an in-depth account of governments' use of digital surveillance technology in times of crisis, using different types of qualitative data. Centered around the COVID-19 pandemic, the thesis comprehensively examines the various processes of regulation and development of a contact-tracing application in Norway. It also explores ways of legitimizing digital surveillance technology through a comparison of the governments' approaches to digital contact tracing during the pandemic in Germany, Norway, and the United Kingdom. Moreover, using survey experimental data the thesis provides empirical evidence of European individuals' attitudes towards government surveillance and privacy, and the causal effect of a pandemic setting on these attitudes, as well as the interaction of various forms of trust.

Theoretically, the thesis makes several important contributions. First, it applies and advances existing theories of regulation to crisis situations. Second, it provides insight into the dynamics of governance capacity and legitimacy in relation to digital surveillance technology in crisis management. Third, it develops the argument that privacy regimes and legacies shape governments' legitimacy strategies of digital surveillance technology, but that these strategies are altered under conditions of crisis. Fourth, the thesis makes a unique contribution by explaining how a major crisis affects citizens' attitudes towards government surveillance and privacy and offers a deeper understanding of various forms of trust in relation to surveillance acceptance in and outside of a major crisis. As civilization advances, the question of the prospects and limitations of governmental control over individuals presents itself under new circumstances, and this thesis sheds light on various aspects of that relationship in a modern, digital world filled with crises and instability.

1.2 Outline

This thesis consists of two parts. The first part starts with a discussion of key concepts and an overview of the central themes in the literature, and how this study contributes to that literature. Thereafter, the research design, data, and methods are presented, and the main methodological assessments are discussed. Next, the four articles are summarized. Finally, a concluding discussion of the findings and the implications of the thesis is presented, followed by reflections on ways forward for future research. In the second part, the four articles are presented in their entirety.

2. Overview of the literature

In this section, I first present relevant concepts related to crisis, technology, and surveillance. Then, I discuss what the trade-off between surveillance benefits and privacy entails, in order to understand what assessments might be expected by different actors in a major crisis like a pandemic. Thereafter, an overview of the main ideas of crisis management in public administration is provided, and the limited attention to digital surveillance technology in this field of study is highlighted. Next, I identify the research gaps in the literature and subsequently describe how each article in this thesis addresses these gaps.

2.1 Crisis, pandemic, and digital surveillance technology

The concept of crisis is fundamental to this thesis. The thesis adheres to the understanding of crisis as "*a serious threat to the basic structures or the fundamental values and norms of a system, which under time pressure and highly uncertain circumstances necessitates making vital decisions*" (Rosenthal et al., 1989, p. 10). Over the past few decades, crises have changed and become increasingly more transboundary, meaning they extend beyond functional boundaries and national borders, and involve high degrees of uniqueness, urgency, and uncertainty (Ansell et al., 2010). This means that modern societies in this day and age face increasingly complex problems and are put under onerous strain, which has made crisis management endemic to modern governance (Boin et al., 2005). A major crisis such as a pandemic is a great risk for modern societies, and a recurrent topicality (Morens and Taubenberger, 2011). Pandemics are hard to predict with regard to occurrence, place of origin, timing, and clinical-epidemiological features. While the current age is an age of drugs and vaccines, the premier action for initial pandemic responses is non-pharmaceutical public health efforts, especially those provided by the government, comprising preventive and informational measures (Morens et al., 2020). This was already well-established before the coronavirus in the COVID-19 pandemic emerged and spread in 2019/2020. The interesting features of this major crisis were its global and immediate impact, deep uncertainty, and long duration. It started as a health crisis, and eventually developed into a long-lasting societal crisis (Boin and Lodge, 2021), which meant that decisions had to be made urgently, with a lack of knowledge about the consequences of the virus, and the consequences of the measures to deal with it.

A measure that was employed worldwide to deal with the pandemic was digital surveillance technologies. These are tools, programs, and software developed to monitor and track individuals, groups, and activities in order to analyze data about them. While a range of different surveillance initiatives were implemented in different countries, such as drones, biometric wearables, and facial recognition cameras (Kitchin, 2020; Mbunge et al., 2021; Vargo et al., 2021; Donelle et al., 2023), the specific technology of digital contact tracing applications (apps) was the one that received the most public attention and scrutiny, and which is the main technology in focus in this thesis.

Digital contact tracing apps are a technology where individuals' smartphones register contact with other individuals' smartphones using an identical or similar tracing app. In pandemic management, they are part of an overall contact tracing system, a critical component of the public health response, which aims to notify individuals that they have been in close proximity to infected individuals (Ferretti et al., 2020; Vogt et al., 2022). During the COVID-19 pandemic, the specific purpose of such apps varied between countries, but it first and foremost concerned tracing the coronavirus and the movement of people. Certain apps were also developed to assess other crisis measures. In some countries, tracing apps allowed for registering visits at restaurants, bars, events, and the like, as a precondition to use these services. Moreover, an important aspect of this type of technology is that it is (often) up to citizens to download and use them, making citizens active contributors to public policies (Fossheim and Lund-Tønnesen, 2023). Thus, the technology is part of emerging innovative forms to solve complex policy issues that are integral to the citizen-centricity in new perspectives on governance in the digital age, such as digital-era governance (Margetts and Dunleavy, 2013) and open governance (Meijer et al., 2019).

When technologies of this kind are developed in times of crisis, they can also be understood as "emerging technologies". These are technologies that are fast-growing and have a relatively high impact in a short amount of time, with potentially ambiguous applications (Abbot, 2012; Rotolo et al., 2015). For these reasons, it is often not clear how they fit into existing legislation or regulatory frameworks and how governments and citizens should respond (Lewallen, 2020; Taeihagh et al., 2021). This particularly applies to digital surveillance technologies, because so many of them involve potential security and control advantages as well as privacy drawbacks. As a result, there is a need to balance these benefits and drawbacks when considering the implementation of surveillance measures.

2.2 The balance of surveillance benefits and privacy in times of crisis

To understand what it means to balance surveillance benefits with privacy and why this can be a complicated effort, we need to know what surveillance means and what privacy means. This can give us a better understanding of the relevant values that might be taken into account when assessing trade-offs, and also what considerations can be expected by different actors – be they governments, regulatory agencies, or citizens.

Surveillance

The topic of surveillance has been extensively researched, with contributions from many of the social sciences as well as the humanities (Ball et al., 2012; Boersma et al., 2014). The most influential understanding of surveillance is that of sociologist David Lyon, who has defined surveillance slightly different over the years[1] (see e.g., Lyon, 2001, p. 2; Lyon, 2006, p. 403; Lyon, 2007, p. 14; Lyon, 2010b, p. 1; Lyon, 2010a, p. 108; Lyon, 2014, p. 2). For this thesis, surveillance is best understood as "*a routine and focused attention to personal details for the purposes of influence, management, care, and control*" (Lyon, 2006, p. 403). To expand on this definition, surveillance is a set of practices, that do not occur at only one point in time and never again, but regularly and not randomly, and which can connect with a variety of purposes (Lyon, 2007). Care[2] and control are elements of particular relevance to crisis situations, as they relate to the expectations citizens often have for what governments ought to do, namely protect from adverse consequences and provide safety and security. Relatedly, it is by the gathering and use of information (e.g., personal information and details collected through some kind of digital technology, as described above) for the stated purposes of care and control that governments seek to reduce uncertainty and enable risk calculations when there is a great sense of threat. Although surveillance is often seen to be malevolent, in this way its intentions may also be benevolent. However, the line between well-intended care and ill-intended control, management, and influence is fine and often implicit.

Collective surveillance can seem like a 21st century or futuristic phenomenon but has existed for as long as human history (Yates and Whitford, 2022). In historical terms, the information

[1] The central features of the definitions are the same, namely systematic attention to personal details for a given purpose (influence and management), but they vary in their inclusion of aspects such as "control", "protection", "care", "direction" and/or "entitlement", and whether the attention is "systematic" or "focused".

[2] I recognize that the inclusion of "care" in the conception of surveillance has been criticized (see Harding, 2018). However, the intention of using a (well-established) definition that includes this element is to demonstrate the variety of purposes and justifications of surveillance, as well as the particular relevance of care in managing health crises.

gathered from surveillance in pre-industrial societies tended to be collected and stayed local, unshared, unrecorded, and difficult to analyze. This stands in contrast to modern surveillance, where multiple measures including digital technology are intensively and extensively used to collect and analyze data about individuals, groups, and contexts (Marx, 2002). While surveillance has often been associated with autocratic regimes, democratic governments are also deeply committed to surveillance. The justifications for these activities have varied over the years, but they include protecting society, citizens, and the state from terrorism, organized crime, cyberattacks and political extremists, and children from predators. General arguments also include that surveillance is the price one must pay for maintaining liberty and security (Ball et al., 2012; Richards, 2012). In modern times, two major events are said to have greatly impacted surveillance perceptions, in addition to the continual and consistent technological changes produced by firms and states. The 9/11 2001 terror attacks provided a catalyst for the monitoring of citizens by the government, and the 2013 Snowden revelations highlighted issues of large-scale surveillance within and outside the US (Lyon, 2015). These events propagated perspectives such as the "surveillance society" (Ball et al., 2012) and "surveillance capitalism" (Zuboff, 2015). Arguably, a third more recent major event is the COVID-19 pandemic. Let us first look at privacy and its related values before discussing the potential trade-offs in relation to this pandemic.

Privacy

Privacy is a difficult concept to define, and philosophers, legal scholars, social scientists, and others disagree about its constituents (Regan, 1995; Solove, 2002). To illustrate, Warren and Brandeis (1890) viewed it as someone's "right to be let alone" and Westin (1967) viewed it as the safeguarding of personal information. For Solove (2006) it is simply impossible to define and should rather be taxonomically mapped and divided into sixteen categories. The issues in defining and grasping privacy are many, and among them are the complexities of accurately translating the word and the idea to other languages and cultures. Nevertheless, there are notions roughly equating to the English concept of "privacy" (UK) in other languages, for example "privatlivets fred" (Norwegian) and "die Privatsphäre" (German) (Bygrave, 2004). Notions in these countries, and Western societies more generally, share many historical roots.

Contemporary privacy conceptions originate from various sources. Going back to Ancient Greece, Aristotle made the early distinction between the public sphere of life and the private sphere of life. Moreover, the spread of Christianity in the Middle Ages, ideas from drafters of the French and American constitutions, and philosophies of Hegel and Mill to name a few

have also shaped modern notions, beliefs, and legislations of privacy, especially in Western societies (see Whitman, 2004; Vincent, 2016; DeCew, 2018). Mill (1859) followed the public/private distinction of Aristotle and applied it more closely to government authority and control over individuals, and Hegel viewed personality in relation to individuality and freedom (Whitman, 2004). An in-depth discussion of the ideas of these writers and others is beyond the scope of this thesis, but suffice to say that in these writings, values and ideas closely related to privacy are considered, such as freedom, individual autonomy, and identity.

These are fundamental values that are often viewed as essential to human life in some ways, and which influence the assessments people make regarding privacy. When something limits an individual's freedom and stops them from pursuing their goals and interests, or violates their personhood, their beliefs about the costs and benefits of giving up privacy (and accepting surveillance) for society and themselves are affected. These complicated aspects and considerations about values make it difficult to understand privacy, but that should not stop us from studying the phenomenon and having some common understanding of what we are thinking about.

With that said, most relevant for this thesis is a definition of privacy that has information at its core, because that is especially important at this point in human history (Smith et al., 2011; Richards, 2021). In the past, *physical privacy* was at the core of the concept, whereas *information* privacy is now the integral constituent (Smith et al., 2011). Accordingly, information privacy is here understood as "*the desire of individuals to control or have some influence over data about themselves"* (Bélanger and Crossler, 2011, p. 1017). Because privacy is about the control or influence over data (e.g., sharing it), it can be seen to bear some sort of value that is not necessarily universal, but that can differ depending on the individual, the situation, and the context (Solove, 2008; Budak et al., 2013). Seen this way, privacy has varying value, and sharing personal data – and by extension surveillance – can provide both benefits and drawbacks. Combining these points with the general ambiguity regarding when and why surveillance can be harmful (Richards, 2012, p. 1935), it becomes extremely difficult to conclude if and when privacy protection or surveillance activities entail positive or negative outcomes (Acquisti et al., 2016, p. 444). Nevertheless, this observation warrants further exploration.

The core of the trade-offs

The issue of attaining surveillance benefits while maintaining privacy is often characterized as a conflict of values. As stated at the outset, it is a classical issue in political science (see e.g., Mill, 1859; Weber, 1922). At a general level, it is on the one hand about nurturing society and maintaining security for societal protection, often seen as a collective action problem. On the other hand, it is about individual freedom and individuals' agency over their own lives without interference. The responses to issues of this kind, be they by government, regulatory agencies, or citizens, are conventionally viewed as "balancing" and reaching "trade-offs" among competing perspectives, goals, and values (Thacher and Rein, 2004).

First, there can be benefits for both the government and individuals when personal information is shared because the government can optimize its systems for citizens to receive better services. If individuals choose not to share, these benefits might turn into what economists call opportunity costs, that is, one misses out on certain benefits, such as personalized and precise (automatic) case processing (Acquisti et al., 2016, p. 445). Second, when personal information is shared, malevolent actors might obtain that information in both legal and illegal ways (e.g., data leaks or hacking) and use the information for other purposes than it was originally collected for. Such information can give undue power to governmental actors who can use it to influence, control, and manipulate citizens (Richards, 2021). At the heart of this lies the concern that surveillance might chill the exercise of the crucial social values discussed above (e.g., civil liberties) and consequently undermine intellectual activities such as thinking and communication about social and political ideas that might be seen as new, deviant or controversial, but which might also advance society (Richards, 2012).

Another notable challenge in the trade-off between the benefits of surveillance and privacy relates to the fact that the immediate benefits of accepting surveillance often are conveyed as measurable: we can observe a reduction in the number of terrorist attacks or criminal activities, while the privacy consequences are rather diffuse, subtle, incommensurable, and might only be felt and experienced after some time. This is because surveillance practices are often implemented in elusive and careful ways of which individuals are unaware, so as to not break social norms about the accepted level of intrusiveness in a society (Richards, 2021). Such practices come about as a result of individuals being inured to violations of privacy, and the limits of acceptable degrees of intrusiveness are continuously challenged when society increasingly depends on digital technology with surveillance implications.

These are the core points in the balancing and trade-offs between surveillance benefits and privacy at a general level. In crisis situations, such as a pandemic, all the difficult assessments about trade-offs are intensified and made more complex, with additional factors coming into play. To reiterate, crises are situations filled with high uncertainty, urgency, and a great sense of threat (Boin et al., 2005; Baekkeskov, 2016) where the demand for information and control is particularly high. Control in such situations is often associated with something positive (Boersma and Fonio, 2018, p. 5) because it implies lower uncertainty and a better overview of consequences. It can, among other things, be achieved by collecting and analyzing personal data about for example movement and behavior patterns. This information can be advantageous for governments to have in order to improve decision-making, provide better services, and introduce more effective crisis measures, which can lead to an increased sense of control, security, and safety for individuals as well as for governments. Here, it is worth noting that the actual control may be an illusion (Richards, 2021, p. 94), but the sense of control can be real.

Because a major crisis is a complex, overwhelming, and unusual situation that individuals can hardly deal with by themselves, citizens may be willing to give up some liberty for a sense of security provided by the government, because the government is likely the only actor with the capacity to deal with such a major threat. Simultaneously, it is a situation where the intentions and consequences of surveillance are unclear, i.e., its impact on control and security, and the restrictions on civil liberties (Trüdinger and Steckermeier, 2017). Thus, individuals must carefully assess the consequences of surveillance in a possibly limited amount of time, for some specified and unspecified purposes, with insufficient knowledge about risks and benefits. Arguably, these assessments are influenced by how much citizens trust the government, and how much they trust each other (Davis and Silver, 2004; Rykkja et al., 2011). This is because trust can be a valuable and expected heuristic instrument to use when there is not sufficient time or information for citizens to foresee and anticipate consequences in future situations (Lewis and Weigert, 1985).

Governments are also faced with challenging assessments and must engage in quite similar considerations about the discussed trade-offs, but for the purpose of building and maintaining governance capacity and legitimacy (Christensen et al., 2016). As stated at the outset, crises can be situations where governments might expand their surveillance power more generally, but they can also be situations where surveillance is merely used as a means to an end: combating the crisis and maintaining legitimacy by using measures that are effective for this

purpose. Legitimacy, a concept elaborated upon more below, in this context concerns not only citizens' perceptions of government and its actions but also other stakeholders' perceptions, including those of regulators (e.g., data protection authorities).

Regulators too are expected to make their own assessments about how intrusive surveillance measures are into citizens' lives, and if practices are within what they deem as acceptable and appropriate – often based on the written law and established standards. Just like citizens and governments, they need to weigh the potential short-term benefits of increased crisis management capacity against the long-term consequences of potentially relinquishing privacy and other related values, while simultaneously safeguarding their own legitimacy by considering others' reactions to their own responses to introduced surveillance measures. Since the function of a regulator such as a data protection authority is typically to advocate for citizens' privacy interests, they may reach different conclusions than a government about the benefits of surveillance.

Overall, these are the most important aspects and considerations in the trade-offs between surveillance benefits and privacy in crisis situations, for citizens, governments, and regulators. On one side, it is about nurturing and protecting society. On the other, it is about maintaining individual freedom and agency and protecting personal information. The ideal for most is to ensure the benefits of surveillance without the cost of violating privacy. However, as discussed, this is not easily achieved. In addition, it is not always the case that governments seek to expand their surveillance powers with malevolent intentions, nor is it always the case that citizens wish to unconditionally safeguard privacy for themselves and their fellow citizens. In the following, I will explain how the ideas about the trade-offs fit into the literature on public administration and crisis management before I specify the research gaps in the literature.

2.3 Government and crisis management

This thesis is concerned with surveillance and privacy predominantly in relation to digital technology in times of crisis and governmental crisis management. Crisis management can be understood as the process in which organizations handle a crisis before, during, and after its occurrence (Boin et al., 2005; Christensen et al., 2016). It is a form of governance where a rapid response is required, involving a range of mechanisms to deal with the crisis. This thesis mainly deals with governmental actors' roles in crisis management but does not exclude

private actors or citizens in this process. This is due to the government frequently being viewed as a key actor in establishing crisis management systems and political-administrative mechanisms such as coordinating resources, regulating activities, analyzing information, and delivering public service when facing major crises that are unique in nature, unlikely, and have a high impact (Christensen et al., 2016).

Over the years, extensive research has been conducted on crisis management in the social sciences, exploring the various aspects of the so-called pre-crisis phase, the crisis itself, and the post-crisis phase (Pearson and Clair, 1998; Boin et al., 2005; Roux-Dufort, 2007; Coombs and Laufer, 2018). In the past, crisis research tended to focus on technical-managerial and strategical aspects about operational decision-making (’t Hart et al., 2001; Rosenthal et al., 2001; ’t Hart and Sundelius, 2013). This was frequently related to security studies, i.e., international relations, conflict and terrorism studies, and safety, i.e., studies of natural disasters, man-made accidents, emergency management, and industrial safety (’t Hart and Sundelius, 2013). In recent decades, there has been a shift in the literature to view crisis management more in connection with public policy and administration, paying greater attention to the policy processes and public institutions in and of crisis management (Boin et al., 2005; Boin and Lodge, 2016). In this regard, one can say that there have been ambitions to connect crisis management more to public administration as a field of study.

This ambition is, among other things, a response to the prevalence of major crises in modern societies, where the idea about the importance of the public administrative apparatus in crisis governance has been resurrected, as citizens still look to government for managing crises (Ohemeng and Christensen, 2022). Current research suggests that context, uniqueness, and degree of uncertainty of the crisis, as well as the structure and culture of government, will matter for governmental crisis management performance (Christensen et al., 2016). It is also noted that any theory of best managing all types of crises does not exist, but that legitimacy is a precondition to ensuring an effective response (Lægreid and Rykkja, 2023). To understand crisis management, then, there is a need to look at the actions of government, as well as how citizens and other stakeholders such as regulatory agencies, assess, support, and evaluate these actions, i.e., the legitimacy of government (Christensen et al., 2016). Citizens and regulatory agencies play a key role in examining whether the legality, ethicality, and appropriateness of crisis measures and policy decisions are congruent or incongruent with existing beliefs and values (Suchman, 1995), and to what extent measures and decisions are understood as success or failure (McConnell, 2011).

Because of its potential to increase governance capacity and legitimacy in crisis management, digital surveillance technology increasingly constitutes a central part of the political-administrative mechanisms for dealing with crises (Boersma and Fonio, 2018). Only recently has this gained scholarly attention, with some attempting to connect (big) data to crisis management (Watson et al., 2017; Boersma and Fonio, 2018; Boersma et al., 2022). This is not surprising, seeing that such technology had not been invented until recently. Comfort (1993) suggested to integrate information technology into crisis management in order to solve complex problems, but this was very much in the infancy of modern digital technology. With the increased availability of data, crisis management systems can be improved, but data availability also gives prominence to new challenges concerning the relationship between the state and its citizens. While it is seen as a core task of the state to protect citizens against adverse consequences (Boin, 2019), not all means to achieve this end are viewed as legitimate by citizens and stakeholders. It is often required that the state deals with a crisis within the frame of what is desirable, appropriate, or proper in socially constructed systems of norms, beliefs, and values (Suchman, 1995), so as to not undermine the legitimacy of public institutions. Nevertheless, as we have seen, disruptive events can be situations where governments (and other actors) expand their surveillance activities by legitimizing large-scale collection, analysis, and use of personal data in uncertain circumstances (Boersma and Fonio, 2018; Eck and Hatz, 2020).

A major crisis such as a pandemic therefore presents a context in which governments and society might want to be open to unknown and unclear ways of dealing with the crisis they face. Consequently, digital surveillance technology in novel forms is expected to be introduced in such situations. However, as explicated above, this is a relatively underexplored phenomenon. This calls for different analytical approaches to understanding surveillance and privacy in connection with crisis management, regulation, policy choices, and citizens' responses than existing ones, to shed light on the classical issue of governments' control over the individual under different conditions.

2.4 Research gaps and how they are addressed

This section describes and explains how articles 1, 2, 3, and 4 address the overarching research question and the three sub-questions. Specifically, research gaps in the intersection of the fields of public administration, crisis management, and surveillance are addressed. Each

subsection below contributes to expounding the overall research gap identified in this thesis, that is, the issue of government control over the individual in relation to the two core conspicuous features of modern society, namely crises and surveillance.

Regulation of technology in crisis

If we are to understand the usage of digital surveillance technology in crisis and crisis management, we need to understand the regulation of it. This is because managing and responding to the introduction of something new is considered one of the tenets of regulation (Baldwin et al., 2010; Black, 2010). Traditional work on regulation (e.g., Nonet and Selznick, 1978; Kagan and Scholz, 1984; Ayres and Braithwaite, 1992; Gunningham and Sinclair, 1999; Coglianese and Lazer, 2003; Baldwin and Black, 2008) has had a substantial impact on both theory and praxis of regulation over the years. In essence, these contributions are centered around a pluralistic approach to regulation, emphasizing a "regulatory mix", involving a range of policy mechanisms. These mechanisms relate to adapting regulation to regulatees' behavior and decisions, and to specific policy goals.

This pluralistic conception has influenced the regulation of *technology* in general, where Mandel (2009) emphasized the need for understanding the governance of technology in a dynamic way, where new governance structures are instituted as technology evolves. Building on this, Roca et al. (2017) accentuated uncertainty in emerging technology, focusing their attention on how the attributes of technology require adaptive regulatory interventions. Even more recently, there have been several attempts at understanding when, how, and why regulation of emerging technology occurs, through various case studies (e.g., Goyal et al., 2021; Lewallen, 2020; Whitford and Anderson, 2020). What these studies have in common is their attention to different sources of uncertainty, albeit primarily related to technological specifics. What they do not pay attention to is the uncertainty or urgency of the situation, i.e., a major crisis, nor how digital surveillance technology is used to address pressing issues as in a crisis. This research gap is addressed in Article 1 in this thesis, which sheds light on the role of uncertainty and urgency in pluralistic and adaptive regulation of digital surveillance technology specifically, and emerging technology more generally.

Use of digital surveillance technology in crisis management

Furthermore, as previously explicated, a core question remaining in the crisis management literature is the function of digital surveillance technology when managing a crisis (Boersma and Fonio, 2018; Hassankhani et al., 2021; Lee-Geiller and Lee, 2022). We can understand

this to concern two aspects: governance capacity and governance legitimacy (Christensen et al., 2016). These two aspects and their dynamic relationship have not received much scholarly attention until the publication of Christensen et al. (2016). Following this publication, and particularly concerning the COVID-19 pandemic, these aspects gained considerable prominence in the literature. To illustrate, governance capacity and legitimacy have been explicitly linked to crisis management of the pandemic in for example Norway (Christensen and Lægreid, 2020), China (Christensen and Ma, 2021), and South Asia (Jamil and Hossain, 2022).

The concepts involve a range of aspects of crisis management. First, Lodge and Wegrich (2014) divided governance capacity[3] into coordination capacity, analytical capacity, regulation capacity, and delivery capacity. In short, it involves primarily formal structural and procedural aspects in the government, but also how those aspects unfold. Second, governance legitimacy is mainly about the relationship between the government and its audiences, such as citizens and regulators (Suchman, 1995). Legitimacy is a complex concept, which in this thesis is applied in slightly different ways as it can relate to different aspects of public policy and administration.

On the one hand, legitimacy can be seen as a property, resource, or asset of an organization (Suddaby et al., 2017). This is a contingency view of legitimacy which understands it as the degree of "fit" between the features, structures, and policies of government, and the expectation of actors in the environment (Meyer and Rowan, 1977). In this view, legitimacy is seen as something the government "possesses". Public administration scholars have divided this conception into three dimensions: input legitimacy, throughput legitimacy, and output legitimacy (Scharpf, 1999; Schmidt, 2013). In short, this concerns citizens' support and acceptance of government action related to participatory quality and politics (input); administrative processes (throughput); and policies and measures (output) (Christensen et al., 2016). What is underexplored in the literature is how the concepts of governance capacity and legitimacy can shed light on the utilization of digital surveillance technology in crisis management. It is also not clear how the outcome of handling crises with digital surveillance technology can be seen as the result of the *dynamics* between governance capacity and legitimacy unfolding during crisis management. For example, high governance capacity can

[3] Lodge and Wegrich (2014) originally wrote about "administrative capacity" and the state's "problem-solving capacity", whereas Christensen et al. (2016) connected these ideas more to crisis management by using the term governance capacity.

lead to high governance legitimacy, and low legitimacy might undermine high capacity. Article 2 investigates these issues, focusing on the development of the contact tracing app in the Norwegian government's management of the COVID-19 pandemic.

On the other hand, legitimacy can be understood as a process, as something that through purposive efforts is constructed and maintained (Suddaby et al., 2017). The basis for this view is that legitimacy is actively and strategically achieved through language use[4] (Neilsen and Rao, 1987; Phillips et al., 2004). In general, agentic approaches of this kind involve rhetorical communication to influence audiences' perceptions (Suddaby and Greenwood, 2005). In crisis management, it entails meaning-making to create and maintain shared understandings of a crisis and ways of dealing with it (Boin et al., 2005; Boin et al., 2009). When it comes to the implementation of digital surveillance technology, these are particularly important processes to analyze. Although crises can create opportunities for governments to implement controversial measures that in more ordinary circumstances would not be conceivable, governments are presumably still required to engage in considerable justification and communication before such technology can gain support and acceptance. We can assume that this applies even if a technology seemingly could contribute to a well-functioning crisis management system, precisely because it might restrain some fundamental societal values.

Some attention has been devoted in the literature to studying this kind of legitimacy work related to surveillance (e.g., Schulze, 2015; Pauli et al., 2016; Tiainen, 2017). These authors have found that there exists a range of legitimacy practices to influence audiences' acceptance of surveillance and that these practices are institutionally embedded. However, this research is conducted in non-crisis circumstances and is not comparative between countries. Understanding legitimizing comparatively is paramount because there is no single best way of managing a crisis or achieving legitimacy (Lægreid and Rykkja, 2023), and because audiences in different contexts will likely expect certain narrative structures by governments based on different historical legacies of practices. This has particular relevance when we are dealing with integral constituents of society such as privacy and other related values, as countries have quite different legacies and regimes of privacy (Bennett and Raab, 2006). Article 3 therefore enquires comparatively into the governmental legitimizing of digital

[4] Some may perceive this as a discursive approach to legitimation (Philips et al., 2004). However, others use terms such as "rhetoric" or "framing" to accentuate the agentic and strategic view of constructing legitimacy and distinguish it from discursive and negotiating interactions (Suddaby and Greenwood, 2005; Suddaby et al., 2017). The thesis follows the latter perspective but recognizes that the influence on public perceptions and interpretations might very well be beyond the malleability of a few actors.

surveillance technology, and how this is shaped by institutional and contextual factors. Specifically, it concentrates on legitimizing digital contact tracing technologies in Germany, Norway, and the United Kingdom during the COVID-19 pandemic, because these countries differ with respect to their privacy legacies, historical practices, and governance arrangements (Bennett and Raab, 2006)

Attitudes towards government surveillance and privacy

I argued above that much remains to be explored about *governments'* use of digital surveillance technology in crisis and crisis management. This also applies to the perspective of *citizens*, and their attitudes towards government surveillance and privacy, and how a crisis might affect those attitudes. Again, if we are to understand the relationship between governments and citizens in modern times, we also need to take this perspective into account. Researchers have addressed citizens' attitudes towards government surveillance and privacy in non-crisis situations (e.g., Dinev et al., 2008; Ball et al., 2012; Friedewald et al., 2017). For example, studies have been concerned with attitudes towards specific surveillance measures (Rykkja et al., 2011; Pavone and Degli Esposti, 2012; Degli Esposti et al., 2021), surveillance policies (Trüdinger and Steckermeier, 2017) and surveillance technologies (West and Bowman, 2016; Bromberg et al., 2018). This research finds that the commonly held assumption that citizens are willing to exchange privacy for security is not always accurate and that this trade-off is dependent on notions of trust, risk, and information. In addition, the context in which surveillance occurs can impact citizens' assessments. At a general level, we know that the sense of uncertainty and sense of threat that crises bring with them can influence citizens' worldviews and beliefs about public policies (Boin et al., 2009; Nielsen and Lindvall, 2021; Vogt Isaksen, 2019). Relating this to privacy and crisis, Davis and Silver (2004) found that after the 9/11 2001 terrorist attacks in the US, citizens were more willing to trade off civil liberties for safety and security the greater their sense of threat.

The insight from these studies on attitudes towards surveillance and privacy is highly valuable and provides us with guidance about the trade-offs between surveillance benefits and privacy in a major crisis. A weakness of these studies is that they are primarily based on correlational evidence and are often conducted in single countries. Experimental data across countries is better suited to understand how a major crisis impacts the extent to which citizens want governments to monitor and track the public or to maintain privacy. Consistent with research approaches in this field (e.g., Davis and Silver, 2004; Rykkja et al., 2011; Svenonius and Björklund, 2018), trust should be considered in a crisis context, for two main reasons. First,

citizens can be unsure about what the implementation of surveillance entails, such as the potential positive impact related to societal safety and control, as well as the negative impact on civil liberties (Trüdinger and Steckermeier, 2017). Thus, when making decisions about whether to accept surveillance or not and to what extent, trust (particularly political trust and social trust) can serve as a useful heuristic (Lewis and Weigert, 1985). Second, major crises are complex situations where the sense of uncertainty, urgency, and threat is high, and where there is a lack of knowledge to assess risks and benefits. In situations like these, one can expect trust to be more important and have a greater association with acceptance of surveillance compared to in more ordinary circumstances (Siegrist and Zingg, 2014). Article 4 seeks to address these issues and answer the third sub-question, using survey experimental data from the European Social Survey from 16 countries and focusing on a pandemic's effect on citizens' attitudes towards government surveillance and privacy and the role of different types of trust.

3. Research design, methods, and data

The thesis employs both qualitative and quantitative methods to answer the research questions. This section first elaborates on the philosophy of science stance of the thesis, and then the case selection processes. Thereafter, the data collection processes, data sources, and analytical approaches are presented. Lastly, I discuss research quality and ethical considerations. Table 2 provides an overview of the research approach, design, and methods of the four articles.

Table 2. Overview of the research approaches in the articles.

	Article 1	**Article 2**	**Article 3**	**Article 4**
Research approach	Qualitative	Qualitative	Qualitative	Quantitative
Research design	Single case study	Single case study (with comparative logic)	Comparative case study	Cross-national survey experiment
Methods	Semi-structured interviews and document analysis	Semi-structured interviews and document analysis	Document analysis	Experiment and multilevel regression analysis

3.1 Philosophy of science

This thesis combines different methods to study the overall phenomenon, thus adhering to what scholars characterize as a pragmatic position to advance knowledge (Tashakkori and Teddlie, 1998; Tashakkori and Teddlie, 2021). This involves a rejection of an either/or school of thought and endorses a pluralistic approach where different theoretical traditions and perspectives are possible, useful, and desired. Accordingly, the logic of inquiry involves both induction and deduction (Johnson and Onwuegbuzie, 2004, p. 18). In this tradition, knowledge is viewed as 1) constructed, and as 2) grounded in the real world. It can be tentative and can change over time.

As this research approach embraces the idea that there are different ways of exploring, describing, explaining, and understanding reality, it follows that both qualitative and quantitative methods can be utilized (Johnson and Onwuegbuzie, 2004). The thesis uses, for example, the power of qualitative studies for illuminating and depicting key aspects and

generating theoretical insight, and the power of large-N designs for analyzing empirical patterns and causal mechanisms (Lieberman, 2005; Moses and Knutsen, 2012, p. 134). The justification for such an approach is that the final output (e.g., this entire dissertation) will be superior compared to that of monomethod studies (Johnson and Turner, 2003). The thesis therefore views these ways of gaining knowledge not as competing or mutually exclusive, but as complementary in political research (Halperin and Heath, 2020, p. 21).

Overall, the pragmatic approach enables the possibility to gain a broad, in-depth, and robust understanding of social phenomena. This is relevant because the use of digital surveillance technology in times of crisis and crisis management is largely understudied, which calls for research approaches from different perspectives building on different schools of thought, involving different methods and data.

3.2 Case selection

Various aspects of the use of digital surveillance technology in crisis management constitute the cases in this thesis. In Article 1, Article 2, and Article 3 the cases concern digital contact tracing apps, designed in the context of public health control during a major crisis, the COVID-19 pandemic. They are unusual cases (Yin, 2014) selected because they provide an opportunity to understand, explore, and explain governmental technology development, crisis management, and regulation and legitimacy of technology in a major crisis situation. A case study approach provides an opportunity to intensively study phenomena empirically, and to uncover and refine theoretical propositions, in order to understand the conditions under which various government efforts occur (George and Bennett, 2005, p. 31). While Article 1 is concerned with regulatory dynamics pertaining to the digital surveillance technology (the contact tracing app) in Norway, Article 2 follows a comparative logic within a single case study by comparing the governmental processes of developing the same app. Norway has a strong state, and regulatory agencies are seen to have high capacity and impact and are structurally separate from parent ministries (Christensen and Lægreid, 2007). We need to keep this in mind when trying to generalize the findings of this thesis on the Norwegian context in particular, as countries have different histories and cultures of privacy and surveillance, and different conditions of governance and regulation. I will revisit these points later in this introductory chapter.

Article 3 is more extensive in its comparative approach by studying legitimizing of the digital surveillance technology in Germany, Norway, and the United Kingdom. These countries all operate under the common EU framework of the General Data Protection Regulation (GDPR) or have a similar version of it, however as stated earlier they differ in several ways in their privacy regime and legacies, allowing for the observation of variation in legitimacy strategies.

In Article 4, the level of analysis moves from the organizational to the individual level. This article analyses experimental survey data of 23,912 individuals across 16 European countries. The countries are selected for the purpose of describing and explaining the effects of a pandemic on European citizens' attitudes towards government surveillance privacy. Implications of the country selection are discussed further below.

3.3 Interviews

One of the central data sources in this thesis is semi-structured interviews. Data from a total of 51 interviews with actors in Norway in various agencies and entities involved in the management of the COVID-19 pandemic were utilized. First, I conducted 16 interviews with key actors who participated in the regulation process and development of the Smittestopp app, the contact tracing app in Norway. They worked in the Norwegian Data Protection Authority (DPA), the Norwegian Institute for Public Health (NIPH), and the public IT company Simula. These interviews were carried out between September 2020 and August 2021, lasted between 30 and 90 minutes, and were recorded and transcribed. By conducting the interviews during this period, I was able to follow the regulatory and crisis management development and changes unusually closely as it evolved. Due to the pandemic itself, all the interviews took place via Zoom.

The selection of these informants was based on their involvement in the regulation process and the development process of the Smittestopp app (which was developed in two versions). Initially, informants were first identified through formal documents from the DPA and the NIPH. Thereafter, snowball sampling was used to identify other relevant actors. Appendix A details the number of interviewees from each organization, and their organizational positions. Furthermore, the interview questions dealt with how the informants understood the pandemic situation, the role of technology in the crisis, related legislation, and how they experienced uncertainty and ambiguity throughout the crisis. The questions also concerned learning from the process of regulating or developing the first version of the Smittestopp app, to the second

version. These interviews made it possible to understand the various phases in the pandemic, related to developing the apps and regulating them, as well as the regulatory conversations that took place in the "shadow" of the formal communication in written documents.

In addition to these interviews, the official and independent Corona Commission in Norway carried out interviews with 35 actors in their first evaluation of the crisis management of the COVID-19 pandemic (NOU, 2021: 6). I relied upon these interviews, with elite administrative and political executives who were involved in the management of the pandemic. These interviews lasted between 60 and 120 minutes and provided valuable insight into the decision-making and assessments made during the crisis and about the use of technology. The actors that were interviewed include the Prime Minister, the Minister of Health, the Minister of Justice, the head of NIPH, and numerous other top politicians and bureaucrats. Appendix B provides a detailed overview of these actors. The interviews are transcribed in their entirety, and available on the commission's website in Norwegian.

3.4 Document analysis

Documents also constitute central data sources and have a variety of functions in this thesis. The documents were analyzed to investigate different aspects related to developing, designing, governing, regulating, and legitimizing the contact tracing apps. They allowed me to gain an overview and in-depth understanding of the management of the COVID-19 pandemic, and the use of digital surveillance technology. By combining documents with interviews in Article 1 and Article 2, it was possible to study the phenomena in different and holistic ways. For Article 3, experience from the Norwegian case provided a useful overview and insight into what type of information and documents were relevant for understanding the ways of legitimizing the tracing technologies in Germany and the United Kingdom.

The data sources include laws and regulatory decisions, expert reports, official press releases, government blogs and reports, transcripts of press conferences and speeches, statements made in the news and on government web pages, annual reports of the Norwegian DPA, and (specific to the case of Norway) the official Corona Commission's first report.[5] All the three

[5] The Part two of the official Corona Commission evaluation was published after the research was conducted for Article 1 and Article 2, but in general expressed the same views regarding use of technology in managing the pandemic as part one.

countries have a relatively transparent public sector, allowing for access to relevant information from the government, departments of health, health agencies, and IT partners.

Statements in the media were typically between a half page and a full page in length, and formal case documents for example in the DPA were typically between 5-20 pages. The Corona Commission's first report was 456 pages long with attachments amounting to more than 1000 pages. This comprehensive report provided extensive insight into the overall crisis management, and the use (or lack thereof) of technology in connection with other measures to deal with the COVID-19 pandemic. Some documents were mainly used to provide vital contextual information to understand the pandemic in general, and the circumstances the informants were situated in (Yin, 2014). This concerns, for example, annual reports for the Norwegian DPA, which were around 100 pages and were utilized to gain an overall understanding of the organization. Those are not necessarily referred to in the articles.

3.5 Assessment of the qualitative methods

There were both benefits and drawbacks with using the different methods. Recollection bias is relevant in research about crisis situations where much is happening simultaneously. To gain precise information of events, I cross-checked information from interviews with information found in documents and interviews with other informants. This was important when trying to understand who said what, when, and why, which can sometimes be unclear in an uncertain and sometimes confusing situation such as a pandemic. With respect to the commission's interviews, the informants read and approved the transcripts of the interviews, allowing informants more time to think about events. Moreover, the involved actors had strong incentives to provide honest and detailed answers, because their responses were reported to the public for scrutiny.

Furthermore, there are both challenges and opportunities with conducting interviews via Zoom (Archibald et al., 2019). A simple challenge is that the conversations do not flow as easily as in person, but this is not seen as a major problem. Rather, the approach has been cost-effective, and practically the only way to conduct interviews during an ongoing pandemic. Additionally, there were some limitations regarding the interviews conducted by the Corona Commission. The main limitation is obviously that I could not ask exactly the questions I wanted but had to rely on the questions posed by the commission. That said, the advantages of getting access to interview data with elite administrative and political

executives which otherwise would be very difficult to obtain clearly outweigh these limitations.

When many decisions are being made and these are extensively documented for public scrutiny, there is a risk of bias in selecting the documents. This is especially so because the governments and specifically the health authorities in the countries published a lot of information about various aspects of the pandemic. While obviously useful, it presented a challenge in handling the volume of documents. To accommodate this, the software NVivo was used to manage the data systematically.

The documents and transcriptions of the interviews were initially analyzed with an open coding process (Halperin and Heath, 2020). Notes were made about the overall themes in the data. Thereafter statements, decisions, and actions were coded and categorized. Coding of the qualitative data was primarily done based on operationalizations of relevant theoretical definitions. Overall, the analysis explored ways in which ideas and concepts provide meaning to social practices related to public administration, crisis management, and digital surveillance technology (Halperin and Heath, 2020, p. 364). In Article 1, this concerns three types of regulatory interventions, in Article 2 decision-making and management related to governance capacity and legitimacy, and in Article 3 three types of strategic legitimizing. Each article details how the individual analyses were conducted.

3.6 Survey experiment

To answer the research question related to citizens' attitudes towards government surveillance and privacy, I used survey experimental data from the European Social Survey (ESS) Round 10. Survey experiments with representative samples enable the testing of causal hypotheses and have a high potential for generalization of the findings to larger populations (Barabas and Jerit, 2010; Mutz, 2011). As with the experimental method more generally, it relies on the use of two groups: one experimental group (which is exposed to a stimulus) and one control group (which is not) (Lijphart, 1971). Subjects are randomly assigned to each group, which are then compared. Any observed differences are subsequently attributed to the intervening stimulus (Lijphart, 1971).

In the tenth round of the ESS, strict random probability sampling was used to attain representative samples of persons aged 15 and over in the 16 countries, in line with standard ESS practice (ESS, n.d.). The pandemic itself impacted the fieldwork of the ESS in that it was

carried out over a longer period than usual, which might create some difficulties for explicit comparisons between countries because attitudes towards surveillance can change over time, based on experience and changing uncertainty in society. The experimental design for each country still holds, however.

The country selection includes those 16 countries that incorporated the voluntary experimental questions in the ESS questionnaire (Bulgaria, Croatia, Czechia, Estonia, Finland, Greece, Hungary, Iceland, Italy, Lithuania, North Macedonia, Norway, Portugal, Slovakia, Slovenia, Switzerland). This resulted in a total of n=11,929 in the control group and n=11,983 in the treatment group. I investigated the acceptance of government surveillance further by looking at the role various types of trust play. Three moderating variables are constructed and/or included in this specific study: political trust, social trust, and trust in the government to deal with the COVID-19 pandemic. How this is done is detailed in Article 4, but it is worth mentioning that multilevel regression analysis was used to account for citizens being grouped in their respective countries (Rabe-Hesketh and Skrondal, 2008).

3.7 Research quality and ethical considerations

Reliability

Reliability refers to the coherence of the collected data during repeated data collection, i.e., repeatability (Yin, 2014). Reliability plays slightly different roles in the thesis, as it involves both qualitative and quantitative methods. In the first three articles, it concerns transparency and trustworthiness in the data collection processes and the analytical procedures (Pratt et al., 2020). This is elaborated upon in the individual articles. The analyzed documents in the thesis are solely public documents and are listed either in the appendices or the reference list of the articles. Also, Appendix A of this thesis shows the organization and the position of those interviewed. Regarding the interviews conducted by the official Corona Commission, the transcripts of these interviews are publicly available to anybody and can be downloaded from the commission's website. Moreover, the survey experimental data utilized in Article 4 is public data, gathered through face-to-face interviews in line with the customary approach of the ESS, and available on the ESS website for anybody to use. The Stata codes are also available upon reasonable request. Overall, because most of the data utilized in this thesis is public, the reliability is high.

Internal validity

Internal validity in this thesis relates to both the qualitative and the quantitative approaches. In the qualitative studies, it refers to the extent to which the findings accurately represent the perspectives, meanings, and experiences conveyed by the informants and the documents (Halperin and Heath, 2020). The amount of data in this thesis is substantial, which has made it possible to enhance validity and generate comprehensive knowledge about crisis management, surveillance, and the pandemic from different viewpoints. This allowed for analytical approaches and conclusions to be assessed against alternative explanations.

In the quantitative study, Article 4, internal validity is mainly about two matters. First, it concerns the meaning of the term "pandemic" that citizens are asked about. An advantage of using the ESS question about a pandemic which is asked *during* a pandemic, is that this increases validity because citizens know what that situation might entail, compared to if a similar question was asked five years before the COVID-19 pandemic. At that time, nobody could have possibly known the actual consequences for themselves or the world. Second, there is a discussion in the privacy literature about what is really measured when asking individuals about their attitudes towards surveillance and privacy. It concerns the potential discrepancy between their "stated" attitudes, and their actual or "revealed" behavior (Solove, 2021). This is commonly known as the "privacy paradox". The thesis assumes that citizens' stated attitudes are their true attitudes but recognizes that actual behavior in terms of choices made about specific privacy and surveillance measures might vary depending on several aspects, such as context, technology, information collected, and so on.

External validity

External validity in this thesis pertains to two types of generalization: theoretical and statistical (Lucas, 2003; Yin, 2014). The first deals with generalizing to broader theory, and the second with generalizations to larger populations (Lucas, 2003). More specifically, theoretical generalization is about deriving new observable implications for theory development, which represents a common objective in crisis research (Buchanan and Denyer, 2013), and serves as one of the objectives of this thesis. The cases are selected precisely to challenge and further advance established theoretical ideas. By developing and testing core analytical assumptions related to regulation, legitimacy, and crisis management, it is possible to apply the analytical approaches in this thesis to other sets of cases and therefore generalize theoretically. For example, idea-based regulatory intervention and the framework developed

in Article 1 can be applied not only to other crises that involve emerging technology and regulatory dynamics, but also to situations that entail uncertainty and ambiguity outside of a crisis context. Moreover, governance capacity and legitimacy and their dynamic interplay can be used to understand the processes of developing and employing other technologies in crisis management in other crises. Additionally, strategic legitimizing of surveillance technology can be applied to analyze the introduction, implementation, and usage of other surveillance technologies and policies across policy areas and country contexts. These analytical approaches must be understood in the context in which they are developed and applied. The countries studied in this thesis operate within the EU's General Data Protection Regulation (GDPR) or a similar legal framework. Surveillance measures policies must generally meet (relatively) strict regulations and standards before implementation, and administrative capacity is generally higher in this region that in other parts of the world. That means that the outcomes of regulation, legitimizing, and usage of digital surveillance technology are expected to vary, but the frameworks and ideas can still be analytically applied in the same way.

Statistical generalization concerns whether inference from samples represents larger populations. In Article 4, sampling is conducted by the ESS with a strict random probability approach, to achieve representativeness for individuals aged 15 and over, in the 16 countries studied. Hence, the findings can be generalized to the population in the selected countries. Another matter is to what extent the findings from the survey experiment can be generalized to other European countries. As the intraclass correlation coefficient in Article 4 indicates that the attitudes towards government surveillance in the 16 countries are influenced by factors that are relatively universal in the region, it is reasonable to generalize findings to other European countries not included in the study. However, because the most populous countries in Europe are not included in the study, some conditions differ. For instance, a potential difference in physical and psychological distance to core political institutions might influence attitudinal dynamics differently in, say, France than in Norway.

That said, importance should be given to the contextual conditions related to major crises. The causal relationship that is established in Article 4 can arguably be generalized to other circumstances that involve uncertainty, threat, and urgency, where the potential threat society faces might exceed the personal burden surveillance can entail. Situations in which this might be the case are humanitarian crises, health crises, terrorism, financial breakdown, war and conflict, tsunamis, hurricanes, climate crises, and energy blackouts.

Ethical considerations

The research in this dissertation was carried out in accordance with Norwegian ethical standards and the "Guidelines for Research Ethics in the Social Sciences and the Humanities" (NESH, 2022). The research design and interview approach has been approved by the Norwegian Centre for Research Data (NSD), now known as Sikt. In the interviews I conducted myself, interviewees were provided information about the purpose of the study and the data collection, what it meant to (voluntarily) participate, and how data about interviewees is protected. The interviewees were also informed at the start of the interview that they could possibly be indirectly identified because not too many actors were involved in the regulation and development processes. Consent to participate was given by all informants. Management of the data from the interviews, which were conducted on Zoom, was carried out according to the University of Oslo's guidelines for doing this.

In the interviews conducted by the official Corona Commission, all the actors were public actors (top administrative officials or politicians), and most of them were subject to the government's instructions, meaning they had a formal obligation to be interviewed by the commission. The others agreed to participate in the interviews (NOU, 2021: 6).

The survey data was collected by the European Social Survey. Participation was voluntary, and all information about respondents is strictly confidential. Data management is conducted in accordance with the EU's GDPR and national data protection laws. The data is stored at Sikt in Norway and is publicly available for anybody to use.

4. Overview of the articles

This chapter provides brief summaries of the four articles in this thesis, and the main results are described. The key similarities and differences between the articles, their contributions, implications, and how they in conjunction answer the overarching research question and the sub-questions are discussed in Chapter 5.

Article 1. Regulating emerging technology in times of crisis: Digital contact tracing in Norway during the COVID-19 pandemic

Published in: *Law & Policy*:

Lund-Tønnesen, Jonas. (2022). "Regulating Emerging Technology in Times of Crisis: Digital Contact Tracing in Norway during the COVID-19 Pandemic." *Law & Policy* 44(3): 278-298. https://doi.org/10.1111/lapo.12195

Article 1 (Lund-Tønnesen, 2022) explores the regulatory interventions employed by regulators when regulating emerging technology in times of crisis. It seeks to understand when and why regulators adapt these interventions. The article provides a new classification and understanding of regulatory interventions that can be applied to understand crisis situations. A differentiation is made between rule-based, norm-based, and idea-based regulatory interventions. While the first two share many similarities with current literature on regulation (e.g., Kagan and Scholz, 1984; Ayres and Braithwaite, 1992; Gunningham et al., 1998; Coglianese et al., 2003; Baldwin and Black, 2008), the third stands out in important ways, focusing on regulatory conversations at a constitutive level of social reality (Black, 2002). It is an expected approach of regulation when information is scarce, rules ambiguous, and situations uncertain (Black, 2002; Gilad, 2014).

These regulatory interventions are analytically applied to the case of regulating the Norwegian contact tracing app Smittestopp, developed during the COVID-19 pandemic. When uncertainty was high at the start of the pandemic, the regulator (the Norwegian DPA) employed an idea-based approach to avoid curbing innovation. As the crisis developed, time pressure intensified, and uncertainty remained high. Because of an insufficient response from the regulated entities, the DPA changed its approach to rule-based and norm-based. Thereafter, a strictly rule-based intervention was embraced, and eventually, this was supported by a norm-based intervention again.

The findings and the analysis in this article provide substantial insight into how different regulatory interventions relate to the different levels of uncertainty and urgency, intra-crisis learning, and the response of regulatees. Crucially, the article demonstrates the importance of idea-based regulation as an essential dimension of analysis to advance our understanding of regulation (of emerging technology) in times of crisis.

Article 2. The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic

Published in: *International Public Management Journal*:

Lund-Tønnesen, Jonas and Christensen, Tom. (2023). "The dynamics of governance capacity and governance legitimacy: The case of a digital contact tracing technology during the COVID-19 pandemic". *International Public Management Journal*, 26:1, 126-144, DOI: https://doi.org/10.1080/10967494.2022.2112328.

Article 2 (Lund-Tønnesen and Christensen, 2023a) analyzes the processes of developing the contact-tracing app Smittestopp in Norway by focusing on its governance capacity and governance legitimacy (Christensen et al., 2016). The study also examines the role of this digital surveillance technology in the crisis management system of the Norwegian government more generally, during the COVID-19 pandemic (Christensen and Lægreid, 2020).

In comparing the various dimensions of governance capacity and legitimacy of the digital surveillance technology (Lodge and Wegrich, 2014; Scharpf, 1999; Schmidt, 2013), the study finds several changes from developing the first version of the app to the second version. For example, the first app was based on low analytical capacity as there was very little knowledge about digital tracing apps worldwide. The app's functionality involved great uncertainty regarding its technical effects, as well as how citizens would respond to such an intrusive measure. Two months after its launch, it was banned by the Norwegian DPA, but a new version was eventually developed. Despite improvements in governance capacity and input and throughput legitimacy, the technology did not enhance the handling of the pandemic in Norway.

We can understand this case in different ways. Legitimacy for an intrusive measure can be difficult to achieve for governments, especially if experts and regulatory agencies have criticized the development process. Moreover, at the time of the second version of the app,

other crisis measures were generally less intrusive in Norway, and they appeared to work satisfactorily, leading to little demand for measures with unclear consequences. Overall, the study highlights the importance of input and throughput legitimacy in addition to output legitimacy for achieving success in crisis management. It also provides valuable insight into the dynamics between governance capacity and legitimacy during a crisis and highlights some important lessons for future crisis management.

Article 3. Privacy regimes, crisis strategies, and governments' legitimizing of digital surveillance technology: Comparing Germany, Norway, and the United Kingdom

Publication status: Sent to *International Journal of Public Administration.*

The literature on legitimizing of surveillance has been concerned with how governments attempt to repair and regain legitimacy after a scandal, specifically related to the NSA/Snowden revelations in 2013 (e.g., Schulze, 2015; Lischka, 2017; Tiainen, 2017; Wahl-Jorgensen et al., 2017; Kuehn, 2018). Less attention has been devoted to how governments attempt to gain and create legitimacy for surveillance in the first place, and whether these ways of legitimizing differ across countries. **Article 3** investigates this, by focusing on governments' legitimizing of digital surveillance technologies in Germany, Norway, and the United Kingdom during the COVID-19 pandemic.

The article distinguishes between three ways of governmental legitimizing based on Suchman (1995): pragmatic, moral, and cognitive legitimizing. It advances this distinction by identifying two core components of each of these approaches. The first component is about the justification of the government's own conduct, while the second component involves direct efforts by the government to convince and persuade citizens to support and utilize the surveillance technology. These are applied in a comparative analysis of the legitimizing of contact tracing applications in the three selected countries.

The analysis shows that all three countries employ the three strategies to some extent, but that there are observable differences. In Germany, the government emphasizes moral values to convince citizens to use the technology, as well as compliance with privacy rules and standards. Norway stresses its own crisis management capacity and cognitive elements, and the UK focuses more on citizens' self-interest. These variations in legitimizing are explained based on institutional path dependencies related to country-specific privacy regime legacies as well as overall strategies for managing the COVID-19 pandemic. For example, Germany's

legacy of taking privacy very seriously, Norway's focus on increasing crisis management capacity, and the UK's accentuation of citizens' self-interest all plausibly explain the variety of approaches. In this way, the article demonstrates the continued existence of different privacy and surveillance approaches between these countries, despite similar data protection laws and expectations of convergence (Bennett, 2018).

Article 4. Attitudes towards government surveillance and the role of trust in a pandemic: A survey experiment in 16 European countries

Publication status: Under review in *Government Information Quarterly*. (co-authored with Christer Flatøy).

What we know about citizens' attitudes towards government surveillance is by and large based on correlational data, but research suggests that crisis situations can influence citizens' acceptance of surveillance (e.g., Davis and Silver, 2004; Rykkja et al., 2011). **Article 4** contributes to this literature by utilizing survey experimental data from the European Social Survey to draw causal inferences about the impact of a major crisis on the acceptance of surveillance and privacy.

The main finding of Article 4 is that citizens in a pandemic setting are more inclined to accept government surveillance compared to citizens outside a pandemic setting. The study further asks if these attitudes interact with three different forms of trust, as trust is a heuristic considered to be important for perceptions of surveillance and privacy (Davis and Silver, 2004; Trüdinger and Steckermeier, 2017). Additionally, because pandemics challenge citizens' capabilities and willingness to make decisions, it is hypothesized that trust matters more for surveillance acceptance in a pandemic setting than in a non-pandemic one (Siegrist and Zingg, 2014).

The study finds that political trust is positively associated with acceptance of surveillance, and that it plays a similar role both in and outside the pandemic setting. It also finds that social trust is negatively associated with acceptance of surveillance, but that this association is less negative in a pandemic, compared to in a non-pandemic setting. Moreover, citizens are more accepting of government surveillance when they trust the government to handle the COVID-19 pandemic. This form of trust is especially pertinent in a pandemic setting. For the two latter forms of trust, we also find interesting differences between low- and high-trusting groups. Overall, this article contributes to understanding the effect of a major crisis on

attitudes towards government surveillance and privacy, and to shed light on that relationship by examining different types of trust in different contexts.

5. Concluding discussion

The overarching theme of this thesis is the issue of the prospect and limits of control and interference government can exercise over individuals in circumstances of crisis and surveillance – two core features of modern societies (Tierney, 2014; Lyon, 2015). At the heart of this issue in lie two competing perspectives that must in some ways be balanced by governments, regulatory agencies, and citizens: the desire for control, safety, and security through surveillance on the one hand, and the preservation of privacy on the other. This section discusses how the thesis answers the research questions presented at the beginning of this introduction chapter that address these issues. I discuss the findings, the implications, and the directions for future research.

5.1 Main findings

In answering the first sub-question *How do governments use digital surveillance technology in crisis management?* I find that digital surveillance technology can play a key role in governmental crisis management but only under certain conditions. Digital surveillance technologies and specifically digital contact tracing apps must be interpreted as a new means to an end, largely untested before the COVID-19 pandemic, that neither governments, regulatory agencies nor citizens fully knew the potential and consequences of. I find that governments seek to utilize such technology as part of an overall crisis management system because of its ability to provide analytical capacity to decision-makers about how a crisis occurs and transpires, and to evaluate the effectiveness of other crisis measures. In such a manner, it is intended to increase overall governance capacity and legitimacy.

Furthermore, it is evident from this study that digital surveillance technology cannot be seen merely as an isolated tool free of value judgements; it must be understood politically. It is part of a system where the expectations of the role of digital surveillance technology are shaped by the past and by the context it is developed in. It may be challenged by actors with objections to its application, particularly actors with privacy concerns. This is also indicated by research about other European countries outside the scope of this thesis (van Brakel et al., 2022). As a tool in crisis management, contact tracing apps must be viewed in connection with other crisis measures. My findings suggest that if other crisis measures are seen as relatively successful, this success can undermine the usage of and reliance on contact tracing apps. In a country with a high-capacity government such as Norway, the effectiveness of this tool can be

difficult to achieve because other measures such as manual contact tracing in municipalities can deliver satisfactory outcomes. This is the case even though this digital technology, in theory, can relieve and be combined with the exhausting task of telephoning citizens by health personnel, as existing research has suggested (Kucharski et al., 2020; Grekousis and Liu, 2021). Therefore, we can imagine that countries with lower governance capacity can benefit more noticeably from the usage of this type of digital surveillance technology in crisis management because it can more easily replace existing weak systems. Whether this is actually the case remains to be seen, and preliminary research has found that successful implementation of digital contact tracing in e.g., developing countries depends on several institutional factors (Arakpogun et al., 2020; Mbunge, 2020). Many developing countries have gained vital crisis management experience with previous pandemics such as Ebola, but also have persistent challenges related to digital infrastructure and political will. Obviously, this varies between countries.

The second sub-question asked *How is digital surveillance technology legitimized and regulated in times of crisis?* Because crises present unique and unfamiliar situations for regulating and legitimizing digital surveillance technology, I develop an analytical framework for how to describe, analyze, and think about the regulation of technology in times of crisis. I differentiate between rule-based and norm-based regulation – a common delimitation in the literature (Ayres and Braithwaite, 1992; Lodge and Wegrich, 2012) – and add a novel way of understanding regulation called *idea-based regulation.* These three types of regulatory interventions are viewed in association with the crisis conditions of uncertainty and urgency.

I apply the framework to the regulation of the contact tracing app Smittestopp in Norway during the COVID-19 pandemic. I found that the Norwegian DPA's regulation of the Smittestopp app occurred in different stages, where the regulator moved from idea-based regulation to a combination of norm-based and rule-based regulation as the crisis developed, depending on levels of uncertainty and urgency. In my examination, it was clear that balancing potential surveillance benefits with privacy in the implementation of the tracing technology was a profound challenge for the regulatory agency. The challenge concerned not only uncertainty related to the technological specifics, as Roca et al. (2017) and Lewallen (2021) stress, but also the context and the problem the technology was developed to assist in managing. In this way, I contribute to the literature on regulating technology (Mandel, 2009; Marchant et al., 2020; Taeihagh et al., 2021), by highlighting specific regulatory challenges under conditions of crisis and in connection with technology involving surveillance.

Regarding the legitimacy aspects of this research question, I explore this from multiple angles. First, I reveal the significance of governance legitimacy's dynamics with governance capacity when digital surveillance technology is utilized in crisis management. They can affect each other, and both are important for a contact tracing app to be used and gain acceptance by citizens and regulators. In this context, I find that seemingly technical choices about technological specifics in a digital surveillance technology can have far-reaching implications for the fate of that measure, as has been suggested in the literature on decision-making in crisis management (Lægreid and Rykkja, 2019). Thus, I show how legitimacy assessments are important to handle carefully by crisis managers from the start of a crisis. Even in a country with a high trust society and a strong state as in Norway, the legitimacy of controversial policy measures cannot be taken for granted when the effectiveness of the policy is contingent on collaboration between citizens and the government.

Furthermore, I examine the strategic legitimizing (Suchman, 1995; Suddaby and Greenwood, 2005; Suddaby et al., 2017) of contact tracing apps by governments in Germany, Norway, and the United Kingdom. The strategies were shaped by the respective countries' privacy regimes and legacies through institutional adaptation, as well as the crisis condition in which the apps were developed. Specifically, I find that these strategies concern how governments in the three countries justify their own choices and attempt to persuade their citizens to embrace surveillance technology by drawing on rhetorical approaches involving pragmatic, moral, and cognitive elements (Suchman, 1995). In short, much of the focus is on moral arguments about protecting society in Germany. In Norway, it is about increasing governance capacity, and in the United Kingdom citizens' self-interest is stressed. The different rhetorical approaches are employed as governments accentuate surveillance benefits, while simultaneously downplaying or avoiding potential privacy drawbacks. By studying approaches to digital surveillance technology this way, I demonstrate empirically the often-held assumption that privacy and data protection practices still differ between countries after the introduction of the General Data Protection Regulation by the EU. Based on these findings, we can expect these practices to differ in other countries and to continue to differ between the three studied countries.

On the whole, these findings contribute to enhancing our understanding of legitimacy in crisis management by illustrating the construct's multifaceted nature (Christensen et al., 2016). They corroborate current research on surveillance that demonstrates that legitimacy strategies are institutionally embedded and that context matters, but also vary more than existing views

on legitimacy suggest (Schulze, 2015; Pauli et al., 2016; Lischka, 2017; Tiainen, 2017). Explicating these governmental responses helps us gain a better understanding of surveillance in crises because it shows how and why governmental actors avail themselves of diverging approaches regarding surveillance and privacy.

In answering the third sub-question *Does a major crisis situation affect citizens' attitudes towards government surveillance and privacy?* I find that a major crisis, a pandemic in this case, does affect citizens' attitudes towards government surveillance and privacy. Citizens are more willing to accept government surveillance at the cost of privacy in a pandemic setting, compared to in a non-pandemic setting. However, my research shows that individuals are still skeptical about surveillance, even if they accept more of it in a pandemic. Interestingly, trust is important for acceptance, which I have already elaborated upon in the previous section on the extended abstract of Article 4. I therefore relate the present discussion to some other aspects of trust and how we should view these findings in a larger perspective.

I find that regarding acceptance of surveillance, the moderation effects of two of the three types of trust included in the study differ significantly between a pandemic and a non-pandemic setting. First, the results show that with increases in social trust, citizens are less accepting of surveillance, irrespective of the setting. However, when investigating different levels of trust, I find that whether citizens are considering a pandemic or not matters less for acceptance of surveillance in the case of lower levels of social trust. For higher levels of social trust, on the other hand, trust is more important for acceptance of surveillance. Second, regarding trust in the government to handle the COVID-19 pandemic, the analysis shows that regardless of whether a pandemic is being considered or not, the acceptance of government surveillance increases as this type of trust increases. But just as with social trust, the setting matters less for acceptance of surveillance at lower levels of trust, and at higher levels of trust it is more important, particularly in a pandemic setting. Political trust does not seem to vary with the setting.

The key finding is based on survey experimental data and is thus a unique contribution to a literature that has primarily based its findings on correlational data (e.g., Davis and Silver, 2004; Rykkja et al., 2011; Trüdinger and Steckermeier, 2017). The inclusion of the three types of trust in relation to attitudes towards surveillance and privacy significantly expands our understanding of trust in several ways. While the above-mentioned (and related) research has also included trust, it has not compared its associations in different settings. The present research demonstrates that we need to understand trust with respect to setting (Siegrist and

Zingg, 2014), and that in situations with high levels of uncertainty, urgency, and threat we need to consider different types of trust, as well as differences between low-trusting and high-trusting groups for acceptance of government surveillance.

In total, these findings help us construct a more complete picture to answer the overarching research question, by considering the perspective of government, regulators, and citizens regarding the balance of surveillance benefits against privacy.

5.2 The balance of surveillance benefits and privacy revisited

I argued previously that balancing surveillance benefits and privacy is a difficult task for any actor, and that this issue is exacerbated in crises. The four articles in this thesis collectively reinforce and support this viewpoint. The uncertainty, urgency, and threat of a crisis make assessments about the short-term and long-term consequences of surveillance incredibly challenging. In this way, the issues are relatively universal for most actors in most contexts: crises in general matter for perceptions about the use of surveillance and the protection of privacy. A crisis pressures all actors – whether they are governments, regulators, or citizens – to make decisions and assessments about consequences and values that are associated with surveillance (e.g., control, safety, and security), and privacy (e.g., identity and freedom). This does not only apply to Europe as in this study, but also to other regions of the world.

However, context also matters. Countries have their own historical legacies, experiences, and institutions that influence choices and attitudes about surveillance and privacy in patterned ways. The relative importance of the above-mentioned values therefore depends on several aspects and differs under different conditions for different actors. For governments, historical roots and legacies of surveillance and privacy (Bennett and Raab, 2006; Boersma et al., 2014) in various ways inform the present of how governments are expected to legitimize the use of digital surveillance technology in times of crisis. Such a measure is not only assessed by different actors with respect to the applicable values and whether it conforms to an acceptable practice of surveillance, but also its relation to crisis management systems more generally. These systems vary across countries, and the usage and benefits of digital surveillance technology depend on how prepared governments are and their ability to adapt to changing expectations during crises (Lund-Tønnesen and Christensen, 2023b).

Regulators, and specifically for this study Data Protection Authorities, have a special mandate to maintain a long-term perspective of the consequences of surveillance and assess its impact

on the fate of privacy. They are therefore particularly skeptical about such practices, perhaps especially in crises as these situations are the ultimate test for core values and principles. The actual impact of their regulatory interventions, however, is expected to vary between countries. In the case of Norway, regulatory capacity is high (Christensen and Lægreid, 2007), meaning that the outcome of interventions might be different in countries where regulatory capacity is lower.

For citizens, crises are extremely onerous situations because they are often not able to handle them by themselves, and therefore might have no choice but to accept the government's surveillance efforts because the government is the only one that can deal with the crisis. Simultaneously, citizens might also genuinely want more surveillance because they seek a greater sense of control and safety for themselves and society. As I have accentuated, the intentions and consequences of implemented surveillance are often unclear (Trüdinger and Steckermeier, 2017), and they are even more unclear in crises. Because of such confusion, citizens do not necessarily rely on utility calculations but rather use heuristics such as trust to determine to what extent they are willing to accept surveillance by their government.

Overall, balancing surveillance benefits and privacy in crisis is a complex endeavor and one that will not become easier in future crises. However, with the theoretical and empirical contributions of this dissertation, we now have a richer understanding of which assessments and responses are made by different actors, and why.

5.3 Ways forward in an age of surveillance

It is evident that digital technology will assume an ever more pivotal role in future crisis management and in shaping future societies (Boersma and Fonio, 2018). Throughout this chapter, one view has been that the collection and analysis of personal data about choices, behavior, and movement can improve services, management of crises, and provide a sense of control. However, this trajectory can also propel society towards a more ominous path, diverging from the optimistic conjectures of surveillance advocates. As Zuboff (2019) describes when discussing surveillance capitalism, the improvement of services by use of personal data can be seen as a first step in predicting human behavior, which eventually enables the influence, manipulation, and control of human behavior. This big data development, for example by use of voter analytics, can have serious consequences for democracy, as seen in the 2016 election in the US and regarding Brexit in the UK (Chester

and Montgomery, 2017). These events might just be the beginning. The norms for acceptable levels of intrusiveness are continuously altered, and actors such as governments and corporations exert pressure to downplay the negative consequences of surveillance because they have something to gain from making citizens believe that privacy is "dying" (Richards, 2021). Having said that, the challenges posed by many digital technologies do not stem from their inherent nature. They stem from the question of who wields control over these tools, and thus who can influence and manipulate others. In an age of surveillance, transparency might gain increased significance by allowing external actors to scrutinize the activities of government.

5.4 Policy implications

One way of overcoming skepticism and disapproval of surveillance for governments is to ensure transparency and facilitate external scrutiny when developing surveillance measures. Providing clarity about intended goals, technicalities, and durations of surveillance from the start can allow external actors – citizens and regulators – to understand why surveillance measures are implemented and offer valuable feedback for improving them. Such transparency can produce more accountable governments and prevent abuse of power, injustice, and corruption (Richards, 2021). Complying with privacy regulations from the outset, such as the GDPR but also future technology regulations that are likely to be implemented, is certainly a minimum requirement.

Moreover, allocating resources to constructing legitimacy alongside these efforts when introducing the policy rather than repairing legitimacy after errors are revealed can ease some of the challenges for governments. Although the findings of this thesis relate to public health and digital contact tracing, the legitimacy of surveillance measures might spill over to other policy areas and measures. Legitimacy (or lack thereof) for one surveillance practice or technology can encourage (or discourage) the introduction of similar surveillance practices and technologies. Politicians and bureaucrats should keep these potential effects in mind when designing the future digital state.

It is in the interest of many that governments continue to explore the advantages that digital technology can provide because there is undoubtedly much untapped potential (Fossheim and Lund-Tønnesen, 2023). As discussed, these technologies can, in theory, often rapidly relieve older and manual systems in crisis management and society in general, and governments

should not shy away from experimentation simply because one specific measure was rather ineffective and received criticism during the COVID-19 pandemic. Simultaneously, it might be wise to not attempt to exploit all crises to introduce dubious surveillance measures. That might weaken citizens' and regulators' confidence in government and cause mistrust.

5.5 Directions for future research

Research on crisis and crisis management has gradually included digital surveillance technology as part of their study (Boersma and Fonio, 2018; Boersma et al., 2022), but there is still much to explore and explain. Future research must investigate the usage of other surveillance technologies that include for example artificial intelligence, algorithms, and big data, to examine their role in improving, impairing, or complicating crisis management. The understanding of these technologies in crisis management and what they mean for governance capacity and legitimacy would benefit greatly from empirical studies in other social and cultural contexts, beyond the European one as in this thesis.

Moreover, much remains to be done to further our comprehension of the regulation of emerging technologies, both theoretically and empirically. Some of the ideas developed in this thesis, for example idea-based regulatory interventions, could be analytically applied to technologies like the ones mentioned above, in other crises and outside of crises. Current research has studied the regulation of technology primarily with qualitative approaches, and future research should therefore apply more quantitative methods to understand regulatory dynamics across a range of policy areas. Lastly, it would be interesting to study attitudes towards surveillance of bureaucrats and politicians who propose and implement surveillance policies and compare those with citizens' attitudes. Are they more willing to use personal data for improving public policies than others? Does policy area matter? Does country-context matter? These questions merit scholarly attention.

6. References

'T Hart, P., Heyse, L. and Boin, A. 2001. Guest editorial introduction. New trends in crisis management practice and crisis management research: Setting the agenda. *Journal of Contingencies and Crisis management,* 9**,** 181-188.

'T Hart, P. and Sundelius, B. 2013. Crisis management revisited: A new agenda for research, training and capacity building within Europe. *Cooperation and Conflict,* 48**,** 444-461.

Abbot, C. 2012. Bridging the Gap – Non-state Actors and the Challenges of Regulating New Technology. *Journal of Law and Society,* 39**,** 329-358.

Acquisti, A., Taylor, C. and Wagman, L. 2016. The Economics of Privacy. *Journal of Economic Literature,* 54**,** 442-492.

Ansell, C., Boin, A. and Keller, A. 2010. Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of contingencies and crisis management,* 18**,** 195-207.

Arakpogun, E. O., Elsahn, Z., Prime, K. S., Gerli, P. and Olan, F. 2020. Digital contact-tracing and pandemics: Institutional and technological preparedness in Africa. *World development,* 136**,** 105105.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G. and Lawless, M. 2019. Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International journal of qualitative methods,* 18**,** 1609406919874596.

Ayres, I. and Braithwaite, J. 1992. Responsive regulation, transcending the deregulation debate. Oxford and New York: Oxford University Press.

Baekkeskov, E. 2016. Same threat, different responses: experts steering politicians and stakeholders in 2009 H1N1 vaccination policy-making. *Public Administration,* 94**,** 299-315.

Baldwin, R. and Black, J. 2008. Really Responsive Regulation. *Modern law review,* 71**,** 59-94.

Baldwin, R., Cave, M. and Lodge, M. 2010. *The Oxford handbook of regulation*, Oxford Handbooks.

Ball, K., Haggerty, K. and Lyon, D. 2012. *Routledge handbook of surveillance studies,* London, Routledge.

Barabas, J. and Jerit, J. 2010. Are survey experiments externally valid? *American Political Science Review,* 104**,** 226-242.

Beck, U. 1992. *Risk society: towards a new modernity,* London, Sage.

Bélanger, F. and Crossler, R. E. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly***,** 1017-1041.

Bennett, C. and Raab, C. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edn. MIT Press, Cambridge, MA.

Bennett, C. J. 2018. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity,* 23**,** 239-246.

Black, J. 2002. Regulatory Conversations. *Journal of Law and Society,* 29**,** 163-196.

Black, J. 2010. 'The role of risk in regulatory processes', in R. Baldwin, M. Cave and M. Lodge (eds) *Oxford Handbook of Regulation*, Oxford, Oxford University Press.

Boersma, K., Büscher, M. and Fonio, C. 2022. Crisis management, surveillance, and digital ethics in the COVID-19 era. *Journal of Contingencies and Crisis Management,* 30**,** 2-9.

Boersma, K. and Fonio, C. 2018. Big data, surveillance and crisis management. *Big data, surveillance and crisis management.* Routledge.

Boersma, K., Van Brakel, R., Fonio, C. and Wagenaar, P. 2014. *Histories of state surveillance in Europe and beyond*, Routledge.

Boin, A. 2019. The transboundary crisis: Why we are unprepared and the road ahead. *Journal of Contingencies and Crisis Management,* 27**,** 94-99.

Boin, A. and Lodge, M. 2016. Designing resilient institutions for transboundary crisis management: A time for public administration. *Public administration,* 94**,** 289-298.

Boin, A. and Lodge, M. 2021. Responding to the COVID-19 crisis: a principled or pragmatist approach? *Journal of European Public Policy,* 28**,** 1131-1152.

Boin, A., Lodge, M. and Luesink, M. 2020. Learning from the COVID-19 crisis: an initial analysis of national responses. *Policy Design and Practice,* 3**,** 189-204.

Boin, A., T Hart, P. and Mcconnell, A. 2009. Crisis exploitation: political and policy impacts of framing contests. *Journal of European public policy,* 16**,** 81-106.

Boin, A., T Hart, P., Stern, E. and Sundelius, B. 2005. *The Politics of Crisis Management – Public Leadership Under Pressure*. Cambridge: Cambridge University Press.

Bromberg, D. E., Charbonneau, É. and Smith, A. 2018. Body-worn cameras and policing: A list experiment of citizen overt and true support. *Public Administration Review,* 78**,** 883-891.

Buchanan, D. A. and Denyer, D. 2013. Researching tomorrow's crisis: methodological innovations and wider implications. *International Journal of Management Reviews,* 15**,** 205-224.

Budak, J., Anić, I.-D. and Rajh, E. 2013. Public attitudes towards privacy and surveillance in Croatia. *Innovation: The European Journal of Social Science Research,* 26**,** 100-118.

Bygrave, L. A. 2004. Privacy protection in a global context–a comparative overview. *Scandinavian Studies in Law,* 47**,** 319-348.

Cayford, M. and Pieters, W. 2018. The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society,* 34**,** 88-103.

Chester, J. and Montgomery, K. C. 2017. The role of digital marketing in political campaigns. *Internet Policy Review,* 6**,** 1-20.

Christensen, T. and Lægreid, P. 2007. Regulatory Agencies—The Challenges of Balancing Agency Autonomy and Political Control. *Governance,* 20**,** 499-520.

Christensen, T. and Lægreid, P. 2020. Balancing Governance Capacity and Legitimacy: How the Norwegian Government Handled the COVID-19 Crisis as a High Performer. *Public administration review,* 80**,** 774-779.

Christensen, T., Lægreid, P. and Rykkja, L. H. 2016. Organizing for Crisis Management: Building Governance Capacity and Legitimacy. *Public administration review,* 76**,** 887-897.

Christensen, T. and Ma, L. 2021. Comparing SARS and COVID-19: Challenges of Governance Capacity and Legitimacy. *Public Organization Review***,** 1-17.

Coglianese, C. and Lazer, D. 2003. Management-based regulation: prescribing private management to archieve public goals. *Law & society review,* 37**,** 691.

Coglianese, C., Nash, J. and Olmstead, T. 2003. Performance-based regulation prospects and limitations in health, safety and environmental protection. Adm. Law Rev. 55, 705-529.

Comfort, L. K. 1993. Integrating information technology into international crisis management and policy. *Journal of contingencies and crisis management,* 1**,** 15-26.

Coombs, W. T. and Laufer, D. 2018. Global crisis management–current research and future directions. *Journal of International Management,* 24**,** 199-203.

Cucinotta, D. and Vanelli, M. 2020. WHO declares COVID-19 a pandemic. *Acta bio medica: Atenei parmensis,* 91**,** 157.

Davis, D. W. and Silver, B. D. 2004. Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American journal of political science,* 48**,** 28-46.

Decew, J. 2018. Privacy. *The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.),* https://plato.stanford.edu/archives/spr2018/entries/privacy *(Accessed September 25 2023).*

Degli Esposti, S., Ball, K. and Dibb, S. 2021. What's in it for us? Benevolence, national security, and digital surveillance. *Public Administration Review,* 81**,** 862-873.

Dinev, T., Hart, P. and Mullen, M. R. 2008. Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems,* 17**,** 214-233.

Donelle, L., Comer, L., Hiebert, B., Hall, J., Shelley, J. J., Smith, M. J., Kothari, A., Burkell, J., Stranges, S. and Cooke, T. 2023. Use of digital technologies for public health surveillance during the COVID-19 pandemic: A scoping review. *Digital Health,* 9**,** 20552076231173220.

Eck, K. and Hatz, S. 2020. State surveillance and the COVID-19 crisis. *Journal of Human Rights,* 19**,** 603-612.

Ess n.d. *Sampling*. European Social Survey. Available: https://www.europeansocialsurvey.org/methodology/ess_methodology/sampling.html (accessed June 1, 2022).

Evan, W. M. and Manion, M. 2002. *Minding the machines: Preventing technological disasters*, Prentice Hall Professional.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. and Fraser, C. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science,* 368**,** 6491.

Fossheim, K. and Lund-Tønnesen, J. 2023. Digitalization of public sector organizations over time: The applicability of quantitative text analysis. *International Review of Administrative Sciences***,** 00208523231183569.

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R. and Peissl, W. 2017. *Surveillance, privacy and security*, Taylor & Francis.

George, A. L. and Bennett, A. 2005. *Case studies and theory development in the social sciences,* Cambridge, Mass, MIT Press.

Gilad, S. 2014. Beyond endogeneity: How firms and regulators co-construct the meaning of regulation. *Law & Policy,* 36**,** 134-164.

Goyal, N., Howlett, M. and Taeihagh, A. 2021. Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework. *Regulation & Governance*.

Grekousis, G. and Liu, Y. 2021. Digital contact tracing, community uptake, and proximity awareness technology to fight COVID-19: a systematic review. *Sustainable cities and society,* 71**,** 102995.

Gunningham, N., Grabosky, P. N. and Sinclair, D. 1998. *Smart regulation : designing environmental policy,* Oxford, Clarendon Press.

Gunningham, N. and Sinclair, D. 1999. Regulatory Pluralism: Designing Policy Mixes for Environmental Protection. *Law & Policy,* 21**,** 49-76.

Halperin, S. and Heath, O. 2020. *Political research: methods and practical skills*, Oxford University Press, USA.

Harding, J. M. 2018. Picking the Speck and Missing the Beam in the Eye of Surveillance: On the Failure to See Eye to Eye with David Lyon. *Surveillance & Society,* 16**,** 554-567.

Hassankhani, M., Alidadi, M., Sharifi, A. and Azhdari, A. 2021. Smart city and crisis management: Lessons for the COVID-19 pandemic. *International Journal of Environmental Research and Public Health,* 18**,** 7736.

Head, B. W. and Alford, J. 2015. Wicked problems: Implications for public policy and management. *Administration & society,* 47**,** 711-739.

Jamil, I. and Hossain, A. 2022. Do governance capacity and legitimacy affect citizens' satisfaction with COVID-19 management? Some evidence from South Asia. *International Journal of Public Sector Management*.

Johnson, R. B. and Onwuegbuzie, A. J. 2004. Mixed methods research: A research paradigm whose time has come. *Educational researcher,* 33**,** 14-26.

Johnson, R. B. and Turner, L. A. 2003. *Data collection in mixed methods research. In A. Tashakkori, and C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research*, Thousand Oaks, CA: Sage.

Kagan, R. A. and Scholz, J. T. 1984. The Criminology of the Corporation and Regulatory Enforcement Strategies. In: K. Hawkins and J. M. Thomas (eds) *Enforcing Regulation*. Bostonm MA: Kluwer-Nijhoff.

Kamel Boulos, M. N., Resch, B., Crowley, D. N., Breslin, J. G., Sohn, G., Burtner, R., Pike, W. A., Jezierski, E. and Chuang, K.-Y. S. 2011. Crowdsourcing, citizen sensing and sensor web technologies for public and environmental health surveillance and crisis management: trends, OGC standards and application examples. *International journal of health geographics,* 10**,** 1-29.

Kitchin, R. 2020. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity,* 24**,** 362-381.

Kucharski, A. J., Klepac, P., Conlan, A. J., Kissler, S. M., Tang, M. L., Fry, H., Gog, J. R., Edmunds, W. J., Emery, J. C. and Medley, G. 2020. Effectiveness of isolation, testing,

contact tracing, and physical distancing on reducing transmission of SARS-CoV-2 in different settings: a mathematical modelling study. *The Lancet Infectious Diseases,* 20**,** 1151-1160.

Kuehn, K. M. 2018. Framing mass surveillance: Analyzing New Zealand's media coverage of the early Snowden files. *Journalism,* 19**,** 402-419.

Lee-Geiller, S. and Lee, T. 2022. How does digital governance contribute to effective crisis management? A case study of Korea's response to COVID-19. *Public Performance & Management Review,* 45**,** 860-893.

Lewallen, J. 2020. Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & governance*.

Lewallen, J. 2021. Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & governance,* 15**,** 1035-1052.

Lewis, J. D. and Weigert, A. 1985. Trust as a social reality. *Social forces,* 63**,** 967-985.

Lieberman, E. S. 2005. Nested analysis as a mixed-method strategy for comparative research. *American political science review,* 99**,** 435-452.

Lijphart, A. 1971. Comparative politics and the comparative method. *American political science review,* 65**,** 682-693.

Lischka, J. A. 2017. Explicit terror prevention versus vague civil liberty: How the UK broadcasting news (de) legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society,* 20**,** 665-682.

Lodge, M. and Wegrich, K. 2012. *Managing regulation : regulatory analysis, politics and policy,* Basingstoke, Palgrave Macmillan.

Lodge, M. and Wegrich, K. 2014. *The Problem-Solving Capacity of the Modern State: Governance challenges and administrative capacities*, Oxford: Oxford University Press.

Lucas, J. W. 2003. Theory-testing, generalization, and the problem of external validity. *Sociological Theory,* 21**,** 236-253.

Lund-Tønnesen, J. 2022. Regulating emerging technology in times of crisis: Digital contact tracing in Norway during the Covid-19 pandemic. *Law & Policy,* 44**,** 278-298.

Lund-Tønnesen, J. and Christensen, T. 2023a. The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic. *International Public Management Journal,* 26**,** 126-144.

Lund-Tønnesen, J. and Christensen, T. 2023b. Learning from the COVID-19 Pandemic: Implications from Governance Capacity and Legitimacy. *Public Organization Review*.

Lyon, D. 2001. *Surveillance society: Monitoring everyday life*, McGraw-Hill Education (UK).

Lyon, D. 2006. Airport screening, surveillance, and social sorting: Canadian responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice,* 48**,** 397-411.

Lyon, D. 2007. *Surveillance studies: an overview,* Cambridge, Polity.

Lyon, D. 2010a. Surveillance, Power and Everyday Life. *In:* KALANTZIS-COPE, P. & GHERAB-MARTÍN, K. (eds.) *Emerging Digital Spaces in Contemporary Society: Properties of Technology.* London: Palgrave Macmillan UK.

Lyon, D. 2010b. Surveillance, power and everyday life. *Emerging digital spaces in contemporary society.* Springer. Retrieved from: https://panoptykon.org/sites/default/files/FeedsEnclosure-oxford_handbook_3.pdf.

Lyon, D. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society,* 1**,** 2053951714541861.

Lyon, D. 2015. *Surveillance after snowden*, John Wiley & Sons.

Lægreid, P. and Rykkja, L. H. 2019. *Societal Security and Crisis Management: Governance Capacity and Legitimacy (eds.),* London, Palgrave Macmillan.

Lægreid, P. and Rykkja, L. H. 2023. Strategic public management in crises. *Handbook on Strategic Public Management.* Edward Elgar Publishing.

Mandel, G. N. 2009. Regulating Emerging Technologies. *Law, Innovation and Technology,* 1**,** 75-92.

Marchant, G., Tournas, L. and Gutierrez, C. I. 2020. Governing emerging technologies through soft law: Lessons for artificial intelligence—An introduction. *Jurimetrics,* 61**,** 1-18.

Margetts, H. and Dunleavy, P. 2013. The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences,* 371**,** 20120382.

Marx, G. T. 2002. What's New About the" New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society,* 1**,** 9-29.

Mbunge, E. 2020. Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews,* 14**,** 1631-1636.

Mbunge, E., Akinnuwesi, B., Fashoto, S. G., Metfula, A. S. and Mashwama, P. 2021. A critical review of emerging technologies for tackling COVID-19 pandemic. *Human behavior and emerging technologies,* 3**,** 25-39.

Mcconnell, A. 2011. Success? Failure? Something in-between? A framework for evaluating crisis management. *Policy and Society,* 30**,** 63-76.

Meijer, A. J., Lips, M. and Chen, K. 2019. Open governance: A new paradigm for understanding urban governance in an information age. *Frontiers in Sustainable Cities,* 1**,** 3.

Meyer, J. W. and Rowan, B. 1977. Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology,* 83**,** 340-363.

Mill, J. 1859. *On Liberty,* London, John W. Parker & Son.

Morens, D. M., Daszak, P., Markel, H. and Taubenberger, J. K. 2020. Pandemic COVID-19 joins history's pandemic legion. *MBio,* 11**,** e00812-20.

Morens, D. M. and Taubenberger, J. K. 2011. Pandemic influenza: certain uncertainties. *Reviews in medical virology,* 21**,** 262-284.

Moses, J. W. and Knutsen, T. L. 2012. *Ways of knowing : competing methodologies in social and political research,* Basingstoke, Palgrave Macmillan.

Mutz, D. C. 2011. *Population-based survey experiments*, Princeton University Press.

Neilsen, E. H. and Rao, M. H. 1987. The strategy-legitimacy nexus: A thick description. *Academy of Management Review,* 12**,** 523-533.

Nesh 2022. Guidelines for Research Ethics in the Social Sciences and the Humanities. . *The Norwegian National Research Ethics Committees.*

Nielsen, J. H. and Lindvall, J. 2021. Trust in government in Sweden and Denmark during the COVID-19 epidemic. *West European Politics,* 44**,** 1180-1204.

Nonet, P. and Selznick, P. 1978. *Law and Society in Transition: Toward Responsive Law,* New York, Octagon Books.

Nou 2021: 6. The Norwegian Government's Management of the Coronavirus Pandemic - Part 1. Norwegian Government. Retrieved December 17, 2022. https://www.regjeringen.no/no/dokumenter/nou-2021-6/id2844388/.

Ohemeng, F. L. K. and Christensen, T. 2022. Guest editorial: Rethinking the state of the administrative state: Is the state back in? *International Journal of Public Sector Management,* 35**,** 373-387.

Oldenhof, L., Postma, J. and Putters, K. 2014. On justification work: How compromising enables public managers to deal with conflicting values. *Public Administration Review,* 74**,** 52-63.

Pauli, R., Sarwary, H., Imbusch, P. and Lukas, T. 2016. "Accepting the Rules of the Game": Institutional Rhetorics in Legitimizing Surveillance. *European Journal for Security Research,* 1**,** 115-133.

Pavone, V. and Degli Esposti, S. 2012. Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science,* 21**,** 556-572.

Pearson, C. M. and Clair, J. A. 1998. Reframing crisis management. *Academy of management review,* 23**,** 59-76.

Perrow, C. 1984. *Normal accidents : living with high-risk technologies,* New York, Basic Books.

Phillips, N., Lawrence, T. B. and Hardy, C. 2004. Discourse and Institutions. *The Academy of Management review,* 29**,** 635-652.

Pratt, M. G., Kaplan, S. and Whittington, R. 2020. Editorial essay: The tumult over transparency: Decoupling transparency from replication in establishing trustworthy qualitative research. *Administrative Science Quarterly,* 65**,** 1-19.

Rabe-Hesketh, S. and Skrondal, A. 2008. *Multilevel and longitudinal modeling using Stata*, STATA press.

Regan, P. M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill, NC.

Richards, N. 2012. The dangers of surveillance. *Harv. L. Rev.,* 126**,** 1934.

Richards, N. 2021. *Why privacy matters*, Oxford University Press.

Roca, J. B., Vaishnav, P., Morgan, M. G., Mendonça, J. and Fuchs, E. 2017. When risks cannot be seen: Regulating uncertainty in emerging technologies. *Research Policy,* 46**,** 1215-1233.

Rosenthal, U., Boin, R. A. and Comfort, L. K. 2001. The changing world of crisis and crisis management. *Managing crises: Threats, dilemmas, opportunities***,** 5-27.

Rosenthal, U., Charles, M. T. and Hart, P. T. 1989. *Coping with crises: The management of disasters, riots, and terrorism*, Charles C. Thomas Publisher.

Rotolo, D., Hicks, D. and Martin, B. R. 2015. What is an emerging technology? *Research Policy,* 44**,** 1827-1843.

Roux-Dufort, C. 2007. Is crisis management (only) a management of exceptions? *Journal of contingencies and crisis management,* 15**,** 105-114.

Rykkja, L. H., Lægreid, P. and Lise Fimreite, A. 2011. Attitudes towards anti-terror measures: The role of trust, political orientation and civil liberties support. *Critical Studies on Terrorism,* 4**,** 219-237.

Scharpf, F. W. 1999. *Governing in Europe: Effective and democratic?* Oxford: Oxford University Press.

Schmidt, V. A. 2013. Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'. *Political Studies,* 61**,** 2-22.

Schulze, M. 2015. Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society,* 13**,** 197-217.

Siegrist, M. and Zingg, A. 2014. The role of public trust during pandemics: Implications for crisis communication. *European psychologist,* 19**,** 23.

Smith, H. J., Dinev, T. and Xu, H. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly***,** 989-1015.

Solove, D. J. 2002. Conceptualizing privacy. *California law review***,** 1087-1155.

Solove, D. J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review,* 154**,** 477.

Solove, D. J. 2008. *Understanding privacy,* Cambridge, Mass, Harvard University Press.

Solove, D. J. 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.,* 89**,** 1.

Suchman, M. C. 1995. Managing legitimacy: Strategic and institutional approaches. *Academy of management review,* 20**,** 571-610.

Suddaby, R., Bitektine, A. and Haack, P. 2017. Legitimacy. *Academy of Management Annals,* 11**,** 451-478.

Suddaby, R. and Greenwood, R. 2005. Rhetorical strategies of legitimacy. *Administrative science quarterly,* 50**,** 35-67.

Svenonius, O. and Björklund, F. 2018. Explaining attitudes to secret surveillance in post-communist societies. *East European Politics,* 34**,** 123-151.

Taeihagh, A., Ramesh, M. and Howlett, M. 2021. Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance,* 15**,** 1009-1019.

Tashakkori, A. and Teddlie, C. 1998. *Mixed methodology: Combining qualitative and quantitative approaches*, sage.

Tashakkori, A. and Teddlie, C. 2021. *Sage handbook of mixed methods in social & behavioral research*, SAGE publications.

Thacher, D. and Rein, M. 2004. Managing value conflict in public policy. *Governance,* 17**,** 457-486.

Tiainen, M. 2017. (De) legitimating electronic surveillance: A critical discourse analysis of the Finnish news coverage of the Edward Snowden revelations. *Critical Discourse Studies,* 14**,** 402-419.

Tierney, K. 2014. *The social roots of risk: Producing disasters, promoting resilience*, Stanford University Press.

Trüdinger, E.-M. and Steckermeier, L. C. 2017. Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly,* 34**,** 421-433.

Van Brakel, R., Kudina, O., Fonio, C. and Boersma, K. 2022. Bridging values: Finding a balance between privacy and control. The case of Corona apps in Belgium and the Netherlands. *Journal of Contingencies and Crisis Management,* 30**,** 50-58.

Vargo, D., Zhu, L., Benwell, B. and Yan, Z. 2021. Digital technology use during COVID-19 pandemic: A rapid review. *Human Behavior and Emerging Technologies,* 3**,** 13-24.

Vincent, D. 2016. *Privacy: A Short History.,* Cambridge, Polity Press.

Vogt, F., Haire, B., Selvey, L., Katelaris, A. L. and Kaldor, J. 2022. Effectiveness evaluation of digital contact tracing for COVID-19 in New South Wales, Australia. *The Lancet Public Health,* 7**,** e250-e258.

Vogt Isaksen, J. 2019. The impact of the financial crisis on European attitudes toward immigration. *Comparative Migration Studies,* 7**,** 1-20.

Wahl-Jorgensen, K., Bennett, L. and Taylor, G. 2017. The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication,* 11**,** 740-762.

Warren, S. and Brandeis, L. 1890. *The Right to Privacy*. Harvard Law Review 4:193-220.

Watson, H., Finn, R. L. and Wadhwa, K. 2017. Organizational and societal impacts of big data in crisis management. *Journal of Contingencies and Crisis Management,* 25**,** 15-22.

Weber, M. 1922. *Wirtschaft und Gesellschaft*. Tübingen: J.C.B. Mohr.

West, J. P. and Bowman, J. S. 2016. The domestic use of drones: An ethical analysis of surveillance issues. *Public Administration Review,* 76**,** 649-659.

Westin, A. 1967. *Privacy and freedom.,* New York: Atheneum.

Whitford, A. B. and Anderson, D. 2020. Governance landscapes for emerging technologies: The case of cryptocurrencies. *Regulation & Governance*.

Whitman, J. Q. 2004. The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal***,** 1151-1221.

Yates, J. and Whitford, A. B. 2022. Surveillance as the Past and Future of Public Administration. *Perspectives on Public Management and Governance*.

Yin, R. K. 2014. *Case study research : design and methods,* Los Angeles, Calif, SAGE.

Zuboff, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology,* 30**,** 75-89.

Zuboff, S. 2019. *The Age of Surveillance Capitalism: the Fight for Human Future at the New Frontier of Power,* London, Profile Books.

Appendices

Appendix A. Overview of interviews by the author.

Organization	Type of actor (position)	Number interviewed
Data Protection Authority	Directors, legal advisers, information officers	7
Norwegian Institute of Public Health	Legal advisers, managers responsible for digital development	5
Simula	Managers responsible for digital development, computer programmers	4

Appendix B. Overview of interviews by the Corona Commission.

Name of actor	Position
Erna Solberg	Prime Minister
Monica Mæland	Minister of Justice and Preparedness
Heidi Heggenes	Secretary General, The Ministry of Justice and Preparedness
Espen Nakstad	Assistant Director of Health
Mari Trommald	Director, The Norwegian Directorate for Children, Youth and Family Affairs
Bjørn-Inge Larsen	Secretary General, The Ministry of Health
Sven Marius Urke	Court Administration
Jann Ola Berget	Court Administration
Elisabeth Aarsæther	Director General, The Norwegian Directorate for Civil Protection
Elisabeth Longva	Head of Department, The Norwegian Directorate for Civil Protection
Camilla Stoltenberg	Director General, the Norwegian Institute of Public Health
Line Vold	Head of Department, the Norwegian Institute of Public Health
Geir Bukholm	Deputy Director, the Norwegian Institute of Public Health
Preben Aavitsland	Senior Adviser, the Norwegian Institute of Public Health
Jan Tore Sanner	Minister of Finance
Hans Henrik Scheel	Secretary General, Ministry of Finance
Bjørn Guldvog	Director General, The Directorate of Health
Bent Høie	Minister of Health
Libe Rieber-Mohn	Director General, The Directorate of integration and

	diversity
Lise Sannerud	Director General, The Norwegian Correctional Service
Jan Erik Sandlie	Deputy Director, The Norwegian Correctional Service
Lars Øy	State Secretary, The Prime Minister's Office
Valgerd Svarstad Haugland	County Governor, Oslo and Viken
Knut Storberget	County Governor, Innlandet
Kjell Ingolf Ropstad	Minister for Children and Families

Dag Thomas Gisholt	Secretary General, Ministry for Children and Families
Jonas Gahr Støre	Leader of the Labour Party and the opposition
Tone Wilhelmsen Trøen	President of the Parliament
Kari Sønderland	Director General, Ministry of Health
Elisabeth Salvesen	Deputy Director General, Ministry of Health
Hege Nilssen	Director General, The Directorate of Education
Guri Melby	Minister of Education and Research
Petter Skarheim	Secretary General, Ministry of Education and Research

Part II:
Articles

Article 1: Regulating emerging technology in times of crisis: Digital contact tracing in Norway during the COVID-19 pandemic

Publication status: Published in *Law & Policy*, 2022, *44*(3), 278-298.

DOI: 10.1111/lapo.12195

ORIGINAL ARTICLE

Law & Policy University of Denver WILEY

Regulating emerging technology in times of crisis: Digital contact tracing in Norway during the COVID-19 pandemic

Jonas Lund-Tønnesen

Department of Political Science, University of Oslo, Oslo, Norway

Correspondence
Jonas Lund-Tønnesen, Moltke Moes vei 31, 0851 Oslo, Norway.
Email: jonas.lund-tonnesen@stv.uio.no

Abstract

In times of crisis, emerging technology can pose major challenges for regulators. They must deal with great uncertainty and urgency related to both the crisis and the technology. To understand such situations, this article studies the revelatory case of privacy regulation of a contact-tracing application called Smittestopp, created in Norway during the COVID-19 crisis. Based on public and organizational documents and 48 interviews, the analysis shows that the Norwegian Data Protection Authority faced several options for regulatory intervention throughout the crisis, and adapted its approach based on intra-crisis experience, regulatees' responses, and different levels of uncertainty and urgency. Building on these findings, the study formulates propositions regarding the regulation of emerging technology during a crisis and regulatory agencies' use of rule-based, idea-based, and norm-based interventions. This study provides insight into how these three types of intervention relate to different aspects of a crisis situation. Furthermore, it stresses the importance of idea-based intervention as a key site of analysis in studying technology that emerges during a crisis.

1 | INTRODUCTION

Research on crises has shown that technologies and innovations can emerge rapidly to overcome the crises in question (Mbunge et al., 2021; Meijer et al., 2019). At the same time, emerging technologies bring about uncertainty, both related to their technological specifics and their

broader societal impacts. During the COVID-19 pandemic, a global mega-crisis with high uncertainty and complexity, digital contact tracing applications (apps) were quickly developed across the world to assist in infection tracking (Ferretti et al., 2020; Whitelaw et al., 2020). Differing views on how to manage and use such technology constitute a highly polarized debate (Abbot, 2012; Mandel, 2009). In times of crisis such as a pandemic, proponents argue for the potential of new technologies to protect human lives, while opponents emphasize uncertainties related to ethics, government surveillance, and long-term privacy implications (Boustead, 2021; Budd et al., 2020; Morley et al., 2020).

This dilemma of technological potential and uncertainty represented a key challenge for the Norwegian Data Protection Authority (DPA) during the pandemic. This regulatory agency had to rapidly evaluate the potential of the contact-tracing app created by the Norwegian Institute for Public Health (NIPH), called Smittestopp ("Infection Stop" in Norwegian), while at the same time considering possible detrimental outcomes related to mass surveillance. The DPA thus had to regulate a new technology under conditions of great uncertainty and time pressure, which is a little-researched context in regulation studies.

Previous research on regulation in non-crisis situations has elaborated on how regulators define non-compliance and analyze moves by regulated entities (e.g., Ayres & Braithwaite, 1992; Gunningham et al., 1998; Kagan & Scholz, 1984), as well as how regulated entities themselves respond to acts by regulators (e.g., Fairman & Yapp, 2005; Gunningham & Kagan, 2005; Winter & May, 2001). These studies, however, are not explicit as to what options regulators face *during* a crisis, or how *emerging technology* is regulated during a crisis. A crisis is a special situation in which regulators are expected to welcome initiatives that can assist in combating the crisis, and thus to apply their interventions differently than they would in more stable circumstances. A crisis also represents an opportunity for regulators to attempt to change the sets of underlying ideas and beliefs that constitute a regulatory field (Black, 2002; Boin et al., 2009; Fligstein, 2001). Using this as a point of departure, this article asks the following questions: which interventions do regulators use to regulate emerging technology in times of crisis? What are the conditions under which regulators adapt their choice of interventions for emerging technologies in crisis?

To answer these questions, this article documents and analyzes the Norwegian DPA's choice of different interventions to regulate the Smittestopp app in 2020–2021. This app, and corresponding ones in other countries, are examples of technology created in a short time frame during a crisis, with uncertainty related to function, data collection, data storage, and long-term privacy implications.

At the outset of the crisis when uncertainty was high, the regulator (the Norwegian DPA) initially utilized what is labeled an *idea-based* intervention to not limit technological innovation of the regulated entities (the NIPH and its assisting app developers, Simula and Netcompany). Due to time pressure and lack of response from the regulated entities, *rule-based* and *norm-based* interventions were embraced in phase two. Thereafter, with reduced uncertainty regarding the technology in question, the coronavirus itself, and the effects of lockdown, the DPA pursued a strictly rule-based approach with the ban of the contact-tracing app in phase three. This forced the regulated entities to create a modified second version, Smittestopp 2. In the final phase, the DPA controlled the new technology with rule-based interventions, but supported these interventions with norm-based elements.

Building on these findings, this study formulates propositions regarding the regulation of emerging technology in crisis and regulatory agencies' use of rule-based, idea-based, and norm-based regulatory interventions. This study provides insight into how these three intervention types relate to different aspects of a crisis. Furthermore, it stresses the importance of idea-based interventions as a key site of analysis in studying technology that emerges during a crisis.

The remainder of the article is structured as follows: First, I define relevant concepts and review the relevant literature in order to provide initial analytical direction for the study.

Second, I present the study's methods and data, which rely on a total of 48 expert interviews and document analysis. Third, I thoroughly describe the COVID-19 crisis and the evolution of privacy regulation throughout it. Finally, I summarize the empirical findings, form propositions, and discuss the study's limitations and its implications for further research into the regulation of technologies that emerge during a crisis.

2 | THEORETICAL APPROACH

2.1 | Crisis and uncertainty

An important premise of this study is the concept of crisis. I follow Boin et al. (2005, p. 5), who define a crisis as "a serious threat to the basic structures and the fundamental values and norms of a system which under time pressure and highly uncertain circumstances necessitates making vital decisions" (p. 5). This means that crises inherently involve dynamic and unpredictable circumstances, complicating decision making and the building of governance (regulatory) capacity (Christensen et al., 2016). Crises include wars, famines, epidemics, large financial downturns, and cyber-attacks, and the effects of crises can be both immediate and long-term (Ansell et al., 2010). Crises can both facilitate and destroy technological innovations (Archibugi et al., 2013; Schumpeter, 1934; Sechser et al., 2019; Talmadge, 2019). For instance, Meijer et al. (2019) show that during a range of different crises, new technologies, applications, and digital networks have been used to create and share information and reduce transaction costs for collaboration. The work of regulators in such situations is characterized by uncertainty regarding social structures, uncertainty regarding technology, and limited time to act (Baekkeskov, 2016; Rosenthal et al., 1989), but with the opportunity to facilitate the use of technology. Uncertain situations are characterized by unknown probabilities (Knight, 1921), where past experiences and strategies can only be applied to a small extent (Ansell et al., 2010); in addition, perceived solutions may be ambiguous, meaning they are incongruent, incoherent, or open to interpretation (Hatch & Erhlich, 1993). The onset of the COVID-19 pandemic had all of these features. Before elaborating on how technology in such circumstances is regulated, it is necessary to state what is meant by emerging technology and how it relates to uncertainty.

2.2 | Emerging technology

The concept of "emerging technology" is broad and potentially ambiguous (Abbot, 2012). Based on an extensive literature review, Rotolo et al. (2015) highlighted five attributes that characterize emerging technology: (1) radical novelty; (2) relatively fast growth; (3) coherence; (4) prominent impact; and (5) uncertainty and ambiguity. In essence, emerging technology involves the application of knowledge in new ways, having a relatively high impact in a short amount of time (Rotolo et al., 2015). One may observe all these characteristics in technologies emerging during crisis, during which uncertainty is even higher than in more stable times. Technologies from completely different sectors may share these characteristics (Perrow, 1984), including technologies that have a physical impact, like nanotechnology, vaccines, and military technology, as well as non-physical technologies such as smart applications, 5G, deep learning, social media, and blockchain. The latter are of particular relevance for the study at hand, as it deals with a digital mobile tracing application.

There is arguably a difference in technological uncertainty during times of crisis compared with more stable times. Due to time pressure, a crisis demands openness to solutions that can combat it, but the high level of uncertainty simultaneously provides an opportunity for regulators to impose ideas and preferences and to create interpretations of ambiguous situations

(Black, 2002; Boin et al., 2009). Technological uncertainty in more stable times is characterized by less demand for immediate solutions and a longer time allowance for regulators to consider alternatives on how to deal with the technology, given the greater degree of contextual certainty.

2.3 | Analytical direction: Three regulatory interventions for crisis

Scholars of regulation emphasize that dealing with the introduction of new products and technologies is a primary objective of regulation (Black, 2010; Mandel, 2009). New technologies generate new difficulties, augmenting the presumed gap between existing statutes and regulations and what is regulated. As a consequence, both regulators and regulated entities can be uncertain about how emerging technology fits with existing rules and legislation (Lewallen, 2020). This is especially relevant in times of crisis (Ansell et al., 2010), where common regulatory approaches (e.g., Ayres & Braithwaite, 1992; Baldwin & Black, 2008; Coglianese et al., 2003; Gunningham et al., 1998) are generally not designed for situations of high uncertainty and urgency (Baekkeskov, 2016). This means that situations like the COVID-19 pandemic may call for other regulatory approaches beyond the more common ones.

One way to view different forms of regulatory approaches and how they deal with emerging technology in uncertain circumstances is through the lens of what are here called *rule-based*, *idea-based*, and *norm-based* regulatory interventions. This differentiation derives from neo-institutional theory, where Scott (2014) introduced a broad framework involving three pillars that describe how institutional elements impact social behavior. Inspired by Scott, the present study's point of departure is that regulatory agencies take on different roles and act as "agents" that attempt to influence and guide the behavior of regulatees through various interventions (Fligstein, 2001; Scott, 2003, 2008). These interventions involve different ways for how rules, ideas, and norms can formally and informally be sustained and imposed (Scott, 2008).

2.3.1 | Rule-based intervention

Rule-based intervention entails explicit investigation and control by regulatory agencies. Derived from the core idea of "command and control," rule-based intervention involves the use of formal instruments such as rule-setting, monitoring, and sanctioning activities to manage technology (Scott, 2014), (Baldwin, 1997). Regulatory agencies that make use of rule-based intervention are clear regarding what regulatee behaviors andwhat attributes of technology they expect. In essence, they sustain "the rules of the game" through the underlying mechanism of coercion (DiMaggio & Powell, 1983). Studies investigating what happens when regulators embrace formal control have been conducted in the areas of environmental regulation (Gray & Deily, 1996), labor regulation (Almeida & Carneiro, 2012), and food regulation (Fortin, 2016).

The main argument for a rule-based approach is that the introduction of laws, regulations, or rules is an act of the state using the force of the law, which helps to reduce uncertainty in two ways (Lodge & Wegrich, 2012): first, by clarifying expectations for all players of the game, and second, by enabling information gathering about regulatee behavior. Clear expectations can create higher levels of accountability, transparency, and consistency in obeying the law. Information gathering can enhance the basis for decision-making related to the monitoring of activities, sanctioning, or incentivizing. This perspective employs the idea that without adequate information, enforcing these rules will not achieve or could possibly undermine their intended objectives.

There are several limitations to this approach, which are amplified in crisis situations. One is the rigidity of rules, which can curb innovation (Lodge & Wegrich, 2012). In this study, this

is a vital point, as regulators arguably should support emerging technology that can help combat a crisis. However, when time is limited, adequate information is difficult to obtain. Additionally, the cost of sustaining ubiquitous bureaucratic monitoring systems with potentially ambiguous rules is high. Sanctioning without sufficient information can also be risky, leading to unintended consequences. The adversarial approach represented by rule-based interventions is generally unwanted by regulators, and is often used as a last resort (Ayres & Braithwaite, 1992).

2.3.2 | Idea-based intervention

Regulation with the idea-based approach derives from what Black (2002) labels "regulatory conversations." These conversations work at the constitutive level of social reality, where regulatory agencies attempt to establish shared understandings through taken-for-granted beliefs (Cornelissen et al., 2015; Phillips et al., 2004). They frame what solutions and problems are conceivable (Gilad, 2014; Goffman, 1974) while also establishing definitions of situations (e.g., "market failure," "compliance," and "privacy violation"; Black, 2002, p. 165). Accordingly, regulatory agencies convey what they deem to be fundamental ideas and beliefs that underlie the interpretations of rules, norms, and target technology in the domain in which regulatees operate and technology emerges.

This type of approach has been used to understand international taxation and compliance (Picciotto, 2015), the regulatory evolution of financial markets in Europe (Thiemann & Lepoutre, 2017), and how the media industry is largely regulated by communication (Ali & Puppis, 2018). Outside the area of regulation, Fligstein (2001) sought to understand how different actors made strategic use of cognitive frames to modify the preferences of state actors in the European Union's (EU) Single Market Programs in the 1980s.

The advantages of idea-based regulation become clear in situations in which constantly keeping track of every actor and new technology becomes overwhelming and costly. When information is scarce, situations uncertain, and rules ambiguous (Black, 2002; Gilad, 2014), an idea-based approach can create certainty and inceptively influence the behavior of regulatees and the properties of technology. This approach differs from ordinary "dialogue," such as restorative justice dialogue (Braithwaite, 2017), in that it has a clear focus on the dissemination of fundamental values, rather than warnings of future inspections or harsher sanctions. It also differs from persuasion or education in that it entails shaping and constructing a specific view of orthodox conduct for technological development (Black, 2002; Picciotto, 2007).

One limitation of the idea-based approach is the fact that altering fundamental beliefs and ideas does not come easy (Barley & Tolbert, 1997), especially in relatively stable situations. Beliefs and ideas may be contested, and regulatees can have enough resources to sustain their existing ideas of technology, making the framing and belief-changing work by regulators more difficult. Changes in beliefs may occur mainly through windows of opportunity (Fligstein, 2001), meaning a crisis must be big enough that existing structures of ideas and beliefs are threatened.

2.3.3 | Norm-based intervention

A third possible style of regulatory intervention occurs through normative appeal (Burby & Paterson, 1993; Tyler, 2021; Winter & May, 2001). This norm-based approach focuses on moral duty and reasonableness (Bardach & Kagan, 2017). Regulators attempt to influence regulatees' behavior by emphasizing the rationale and appropriateness of specific laws and regulations, and by reinforcing norms (Gezelius & Hauck, 2011). This intervention is based on social values

and focuses on shaming and praising regulatees. Shaming and praising come about when regulators convey information about expected conduct, establishing what constitutes "good" or "bad" behavior and thereby influencing regulatees' reputations (Bach et al., 2021) and perceived legitimacy (Rorie et al., 2018). Studies of regulators working through appeals to moral duty, appropriateness, and reasonableness have reported increased compliance, for instance in the context of environmental regulation (Winter & May, 2001) and tax regulation (Schwartz & Orleans, 1967).

One advantage of the norm-based approach is its distinct focus on regulatees' duties with respect to specific rules and laws, which creates social expectations. Praising and shaming provide clear signals to regulatees about how they should continue their work. By being less specific beginning at the formative stage regarding what technological attributes are expected, this approach remains open to new technologies (Hagemann et al., 2018).

One challenge with this approach is the difficulty of evaluating which social values are more or less important during a crisis (Boin et al., 2005). For instance, one can expect that determining the tradeoff between ensuring people's privacy and saving human lives involves a complex calculation (Akinsanmi & Salami, 2021). Additionally, emphasizing the reasonableness of rules and shaming or praising behavior can be difficult when some rules are only ambiguously applicable to a given emerging technology.

2.3.4 | The interplay between the regulatory interventions in crisis

The essentials of each intervention are summed up in Table 1. The table describes the three regulatory interventions and their relation to the two key features of crisis situations discussed above: uncertainty and urgency (Boin et al., 2005). Both features are expected to play a role when regulators make decisions about interventions during a crisis. The indicators in Table 1 provide direction for what I will look for in the empirical analysis to observe the different types of regulatory intervention.

All three intervention types involve influencing the behavior of regulatees, particularly with respect to emerging technology. They move along a spectrum from enforcing rules to shaping taken-for-granted ideas, and can potentially reinforce, complement, or interfere with each other (Scott, 2014). For instance, sanctioning can lead to public shaming, and the content of idea-based regulatory conversations can at times appeal to moral duties. Similarly, shaming and sanctioning can cause regulatees to change taken-for-granted ideas, which is more in line with idea-based regulation. However, rule-based interventions can also lead to an adversarial relationship between the regulator and regulatees, which can interfere with idea-based regulation (Black & Baldwin, 2010).

Overall, regulation in crisis situations is complex. Uncertainty concerning the crisis and technology, as well as how the levels of uncertainty change over time, creates a dynamic and unpredictable setting for regulatory agencies. The above discussion provides some initial direction as to how the regulatory interventions may relate to levels of uncertainty, time pressure, and regulators' experience with regulatees' responses. The empirical section of this study seeks to explore how these aspects may relate to one another.

3 | METHODS AND DATA

This is a single case study of privacy regulation concerning a specific technology, Smittestopp, operating within the context of public health control during a crisis. This can be considered a revelatory case (Yin, 2014), meaning that it is illustrative of technology regulation during a crisis, a hitherto relatively unexplored phenomenon. The case was selected with the goal of

TABLE 1 Overview of regulatory interventions in crisis situations

Regulatory intervention	Definition	Indicators	Relation to uncertainty	Relation to urgency
Rule-based intervention	Regulation using formal instruments in line with command and control.	Enforcement, control, sanctions, incentives.	Rigid rules may curb the innovation and technological development needed to combat a crisis. Needs clear rules to enforce.	May take too long to be applied when rules are ambiguous. Used as a last resort if uncertainty is too high over an extended time-period.
Idea-based intervention	Regulation through communication of fundamental beliefs and ideas.	Informal conversations and framing of fundamental beliefs and ideas (general and context specific).	Suitable in situations of high uncertainty.	The communication of ideas and beliefs can be accomplished quickly, even with ambiguous rules. Long-term impact may be unclear.
Norm-based intervention	Regulation that emphasizes moral duty and reasonableness.	Communication of duty, reasonableness, and shaming/praising.	Requires some knowledge about regulatees' activities and technology. Needs somewhat clear rules to know which reactions are relevant.	Can work faster than rule-based intervention as formal case processing is not required.

Note: Own compilation, drawing on Lodge and Wegrich (2012), Black (2002), and Bardach and Kagan (2017).

depicting key aspects of the regulation of emerging technology and understanding how and under what conditions regulation in such special situations occurs. To do this, I provide rich empirical descriptions of how regulation evolved over time and consider perspectives from both regulators and regulatees. This provides the basis for the general propositions concerning the regulation of technology in times of crisis presented in the concluding section of the article.

Documents and interviews constitute the main sources of data for this study. The documents depict the formal communication between the regulator and the regulated entities and are publicly available, reflecting a context with high transparency regarding public sector decision-making. Moreover, the organizations provided additional information through evaluation reports and press releases about their reasoning concerning their regulatory decisions (DPA) and technological development (NIPH and Simula). To clarify, Simula is a public research organization in Norway that provided technical assistance to NIPH as it developed Smittestopp 1. For Smittestopp 2, NIPH received assistance from a private firm called Netcompany.

Government statements and reports provide information about the coronavirus crisis in general, the apps' role in the overall management of the crisis, and relevant laws and regulations. One particularly rich source of information is the first official evaluation report by the Norwegian Corona Commission, which is 456 pages long (see Kvinnsland et al., 2021).

Additionally, the data comprise 48 interviews with actors in various organizations involved in the management of the COVID-19 pandemic in Norway. Sixteen semi-structured interviews were conducted by the author with central actors involved in the regulation process from DPA, NIPH, and Simula. The main criterion for selecting informants was the actors' direct involvement in the regulation process, either as a regulating party or a regulated party. A second

criterion was that informants should have a range of roles in their respective organizations in order to provide different perspectives on the pandemic and the regulation process.

The informants from the DPA were specifically selected because they played a central role in regulating the Smittestopp app (through conversations with regulated entities, in the formal case processing, and in the sanctioning of the app). The informants were first identified through the formal documents, which are publicly available on the websites of DPA and NIPH. Furthermore, I used snowball sampling to find other actors who were involved or who could provide interesting insights into the regulation process but who were not explicitly mentioned in the publicly available documents. Within the DPA, interviewees included legal advisers, information officers, and directors. Interviewees from Simula were computer programmers and managers responsible for developing the app, while interviewees from NIPH included legal advisers and managers involved in or responsible for the development of Smittestopp 1 and 2. Overall, seven interviews were conducted at the DPA, four at Simula, and five at NIPH. The interviews lasted between 30 and 90 minutes, and were recorded and transcribed. Due to the nature of the crisis itself, all interviews took place via Zoom between September 2020 and August 2021. This time-period provided an opportunity to follow the regulatory development with special proximity, and to see the changes that occurred in the transition from Smittestopp 1 to Smittestopp 2.

In the semi-structured interviews conducted by the author, the interviewees were asked to describe how they understood the crisis situation, relevant legislation, the role of technology and privacy in the pandemic, and how they experienced uncertainty and ambiguity throughout the crisis. They were also asked what lessons could be learned from the process of developing or regulating both the first and the second Smittestopp apps. The interviews provided valuable insight into the regulatory conversations that took place prior to the formal communication and the written documents, as well as into other phases of the regulation process.

In addition, the independent official Corona Commission in Norway conducted 32 interviews as part of its evaluation of the Norwegian government's overall management of the COVID-19 pandemic. These interviews offer very rare insight into the overall crisis management approach of the government and the role that technology played in dealing with the pandemic. The interviews were conducted with political and administrative leaders who were key decision-makers during the pandemic, and the transcripts are available to the public (in Norwegian) on the Corona Commission's website (see Corona Commission, 2021). Examples of actors who were interviewed include the head of NIPH, the Minister of Health, the Prime Minister, and leaders in other prominent public health organizations. These interviews lasted between 60 and 120 minutes and provide an understanding of the overall management of the crisis, as well as considerations, goals, and evaluations related to digital contact tracing.

Lastly, I attended public digital conferences and meetings with the Norwegian DPA, NIPH, Simula, and other experts in the field (see NBT, 2020; PrivacyRules, 2020; Simula, 2020a; Tekna, 2020). This allowed me to observe how some of the actors and experts talked to each other about the crisis and about Smittestopp.

The data as a whole cover the government's general crisis management approach as well as information exchanges between the DPA and NIPH (or the assisting developers) that took place between March and December 2020. Appendix A provides an overview of the data sources used in the study.

The documents and the transcriptions were initially analyzed with an open coding process looking for recurrent themes. Early on, it became clear that the different types of regulatory intervention could be organized into various phases. From there on, relevant evidence and statements were categorized into different phases. By specifically looking for the indicators derived from the three types of regulation that gave initial direction to the analysis, I was able to observe the dynamics between the different types of intervention.

The different indicators were found partially in different types of data. The rule-based aspects were found predominantly in written documents, as they are formal interventions, but

the interviews also provided a better understanding of these decisions. As expected, the idea-based aspects occurred during conversations between the different actors, as revealed by the interviews. The norm-based aspects appeared in written documents as explicitly mentioned values around shaming and praising behavior.

I analyzed my own interviews in conjunction with the documents from the DPA and NIPH by comparing and tracking the different perspectives on regulation, uncertainty, technology, and privacy in the different phases. These perspectives were considered in relation to the regulatory interventions decided upon by the DPA. Furthermore, I analyzed the data from the Corona Commission (report and interviews) to gain an informed understanding of how central actors in the government and NIPH perceived uncertainty with regard to the overall management of the crisis and which measures were considered and prioritized in dealing with the pandemic. I then analyzed the role that the Smittestopp app played during the pandemic, as well as the role it could have potentially played, as perceived by the central actors in the government. This was essential for understanding what pressure the DPA experienced while making decisions, what evaluations they had to make, and whether their regulatory efforts were successful.

Overall, the data analysis enabled me to gain a comprehensive understanding of the different perspectives on regulation during the crisis held by both the regulating agency, the DPA, and the regulated entities, with NIPH at the forefront, as well as what assessments were made under these circumstances.

4 | EVOLUTION OF PRIVACY REGULATION THROUGHOUT THE COVID-19 CRISIS

COVID-19 was first detected in China in December 2019. It quickly developed into a highly complex mega-crisis involving the entire world, with governments facing difficult trade-offs between health, economics, and human rights. In Norway, the first confirmed case of infection was registered on February 26, 2020. On March 12, the Norwegian government introduced intrusive control measures, and NIPH began development of Smittestopp 1. The government declared the situation under control on April 6 (Kvinnsland et al., 2021). Table 2 summarizes the course of events in Norway.

Before going into more detail on the different phases of the crisis, I will first provide some background information about the general mission of DPAs and about the development of Smittestopp 1 and 2 in Norway. DPAs were created in many European countries throughout the 1970s, 1980s, and 1990s along with the diffusion of data protection legislation, although several non-European countries now also have similar regulatory agencies (Bennett & Raab, 2020). These agencies go under various names, and in some countries, such as the United States, there is no single authority on privacy or data protection.

The Norwegian DPA shares its formal mission with all EU DPAs, which is to regulate data privacy through the EU General Data Protection Regulation (GDPR). The GDPR was implemented in 2018 and aims to strengthen and harmonize privacy regulation in the processing of personal data across the European Union. It intends to give citizens more control of their own personal digital information and strengthens financial sanctions for cases of non-compliance. DPAs often take on various roles in their task of regulating data privacy, playing at various times the role of consultant, policy adviser, educator, or enforcer (Bennett & Raab, 2020).

The Smittestopp app was developed in two versions, Smittestopp 1 and 2. NIPH had assistance from Simula in developing the first version, and from Netcompany in developing the second. Both apps' primary function was to assist human contact-tracing by tracking the movement patterns of citizens in order to limit the transmission of COVID-19 (Simula, 2020b).

TABLE 2 Overview of 2020 events and regulatory action taken during the COVID-19 pandemic in Norway

Date	Action
March 12	Initiation of extensive infection control measures in Norway and the start of Smittestopp 1
March 27	Regulations issued on digital infection detection
April 4	Expert group announced
April 6	Virus transmission considered under control by Norwegian government
April 9	Expert group preliminary report
April 16	Launch of Smittestopp 1
April 27	Formal inspection by DPA
May 8	First formal letter from DPA to NIPH
May 18	Expert group delivers final report
May 19	DPA formally demands answers from NIPH
June 1	Initial answer from NIPH
June 8	NIPH sends missing information
June 12	Notification of coming ban
June 16	Deactivation of Smittestopp 1 by NIPH
July 6	Official ban of Smittestopp 1 by DPA
September 28	Project start for Smittestopp 2
October 15	DPA formally investigates Smittestopp 2
December 21	Launch of Smittestopp 2

After citizens downloaded the app on their smartphones, the app would notify them once they had been in close contact with someone who reported having been infected by the coronavirus.

Smittestopp 1 worked using both Bluetooth and GPS to track the virus and detect other users (NIPH, 2020a). The information collected by the app was stored centrally at the NIPH for 30 days for research purposes (Simula, 2020b). In Smittestopp 2, GPS tracking was removed, and data was decentralized, being stored only on users' phones. Additionally, open-source code was used in the development of Smittestopp 2; Smittestopp 1 had been closed source.

The significance of open-source code is that the source code of the technology is publicly available for anyone to review and suggest improvements (Fitzgerald, 2006). However, this does not mean that anyone can change the code itself. Closed source, on the other hand, means that the code cannot be accessed by anyone other than the developers themselves. In general, there are advantages and disadvantages to both modalities. However, one can imagine that if a technology is controversial, having open-source code could contribute to transparency, which might be needed to legitimize such an intrusive measure.

4.1 | Phase 1: Development of the crisis and the emergence of new technology

NIPH was not the only actor in the world creating such apps. Computer developers across the world were experimenting with a variety of alternative technologies (Grekousis & Liu, 2021). As these types of technologies were entirely new, at least in a Western context, neither the public, computer developers, nor regulators knew exactly how they would work. This meant that there was no blueprint for how regulators should respond to such technology and no experience on which to base decisions. During the introduction of Smittestopp at the beginning of the crisis, the head of the DPA emphasized the agency's initial communicative approach: "we had a

dialogue with the Norwegian Institute of Public Health and the app developers about privacy impact assessments, about risk and vulnerability analysis, but we only gave verbal input." At this early stage, the DPA also stressed to NIPH and Simula the importance of "privacy by design" (Interviewee 6), meaning that any privacy measures should be built into the technology from the start and integrated throughout the entire technological development process, rather than simply implemented post-development. This was seen as a proactive measure, necessary to ensure privacy and to allow citizens to gain control over information about themselves. In these conversations, NIPH replied that they wanted more understanding from the DPA regarding the urgency of the situation and the overall infection control assessments (Interviewees 29, 30). For instance, a central actor at NIPH said that "we were not able to convince the DPA that we would eventually introduce the necessary privacy measures, but we had them on our list" (Interviewee 12). These included data minimization, reducing data storage time, and assessments of technology change, meaning privacy by design. This indicates that the DPA attempted to impose its ideas upon NIPH/Simula, and that NIPH/Simula resisted by trying to defend their own choices.

The DPA emphasized the importance of transparency, showing all stakeholders that whatever technology was to be involved must be available for outside expert review (Interviewees 6, 9). In a press release on the DPA's website in March (DPA, 2020a), the head of the DPA stated two essential ideas they had communicated:

> In order for citizens to download the app, there must be full transparency from the authorities. Openness builds trust, and only then will more people use the solution. But it is an intrusive measure that the state is now taking in this very special situation. This type of legislation is only legal if it constitutes a necessary, suitable, and proportionate measure in a democratic society.

These are general encouragements, reminding regulated entities and society at large about what fundamental values are at stake. Transparency is seen as a precondition for trust in political institutions and for a democratic society. Additionally, in the same press release, the DPA strongly emphasizes voluntary usage of the app, as well as information about how citizens can withdraw consent (DPA, 2020a).

4.2 | Information in the early stages of the pandemic

In March and the start of April, information was scarce about both the app and the virus. The first written source for understanding Smittestopp was found in the specific regulation mandating its creation (RDI, 2020). The text of the regulation text is relatively short and was issued by the Ministry of Health and Care Services (MH) on March 27. It states that the app's purpose is to surveil citizens in order to monitor the spread of infection and to assess the effect of infection control measures (Kvinnsland et al., 2021). The regulation further declares which data are relevant in monitoring infection spread, and who has access to these data (RDI, 2020). The text of the regulation has very little information about the actual technology, meaning it did not contribute significantly to enhancing the DPA's knowledge.

Recollecting past events, a director at Simula stated in an interview that this regulation was specifically written for Smittestopp by the MH (Interviewee 3). In hindsight, this appears to give a false sense of unambiguous rules. According to informants in the DPA, as the MH had not significantly involved the DPA in this process, the regulation conflicted with existing privacy laws (Interviewees 5, 7). Further illustrating the ambiguity of rules at the start of the crisis, in an online debate with the DPA in June 2020, the director at Simula declared, "the DPA focuses

on laws, we focus on realities" (NBT, 2020). This suggests that the regulatees found the privacy laws in general to be somewhat ambiguous—even rules that were tailored for themselves. This is also in accordance with the perceptions of all tracking apps, where the ethical and legal boundaries are generally unclear (Gasser et al., 2020).

Eight days after the institution of the regulation, the MH assembled an expert group to assess privacy and security issues related to personal information on the app, which had yet to be launched (Expert-Group, 2020a). Due to lack of time, the expert group focused only on security and not privacy in its preliminary report, which was delivered just 5 days after the groups' formation. Thus, the group's findings did not help to reduce uncertainty for the DPA. The group claimed that privacy would be easier to analyze once larger parts of the system were finished (Expert-Group, 2020a). This evaluation made the DPA more suspicious, as the agency could not know whether any privacy measures were included at this early stage. Without any assessments of potential privacy concerns, Smittestopp was launched to the public on April 16. At this point, neither the DPA nor the public had access to risk analyses, privacy assessments, or the protocol documenting the developmental stages of the app.

4.3 | Phase 2: No change in technology

Eventually, the DPA realized that it had not been successful in changing the behavior of the app developers or the trajectory of the technology, as far as it knew. According to the head of the DPA, the agency saw that its way of employing informal communication had not adequately achieved its goals (Interviewee 6). This convinced it to change interventions. Too much time had passed without the DPA knowing what the app developers were up to (Interviewee 6).

On April 27, the DPA announced that it would initiate formal inspections of Smittestopp (DPA, 2020b). By this point, approximately 1.5 million (out of 5.4 million) Norwegians had downloaded the app (NRK, 2020a). The DPA retrieved three types of documents from the developer: privacy impact assessments, risk and vulnerability analyses, and the processing protocols. These documents were examined closely because they show precisely what considerations were taken regarding privacy by NIPH. The DPA found that there were clear shortcomings in the risk and vulnerability analyses, and that the processing protocol was not explicit about what personal data were processed by the application and for what purposes (DPA, 2020c).

After the start of the formal inspection, communication between DPA and NIPH became formal and written, and informal conversations ceased (Interviewees 9, 12). In a letter on May 8, the DPA told NIPH that it would instruct them more thoroughly, in different stages (DPA, 2020d). With this letter, the DPA went through the relevant general laws and privacy laws in detail, specifying their basic principles and appropriate applications. By initiating the investigation, the DPA displayed its skepticism, and the decision received media attention (NRK, 2020b). The DPA was active in media debates around privacy and provided justifications for the investigation, which can partly be interpreted as public shaming of the app. A central actor in Simula said in an interview that some personnel felt that this project was lost due to the negative media attention (Interviewee 3).

Eleven days later, on May 19, the DPA formally requested answers from NIPH with a deadline of June 1. The questions the agency demanded answers to concerned the specific purposes of the personal data collected in the app, current results, the justification for using GPS data and not just Bluetooth data, the justification for central storage of data rather than decentralized storage on citizens' phones, and the usefulness of the application in its current state and at that point in the COVID-19 pandemic (DPA, 2020d, pp. 8–10).

Meanwhile, the expert group completed its report on May 18. Its conclusions were that privacy was not properly ensured on the app, and that data minimization could be achieved. The

group was clear in recommending the use of open-source code in order to allow citizens to know what type of information was collected and as a measure to ensure the protection of private information (Expert-Group, 2020b). This gave the Norwegian DPA some idea about what type of technology it was dealing with. Additionally, the expert group proposed changes to the original government regulation for the app, confirming the uncertainty that the DPA experienced and the ambiguity that NIPH/Simula experienced.

4.4 | Phase 3: answers and action

On June 1, the DPA received answers to some of its questions from NIPH. However, the DPA demanded more documentation on June 8, as the initial documents were not considered to be sufficient, something NIPH disagreed with (Interviewee 15). Four days later, on June 12, the DPA notified NIPH that it would temporarily ban Smittestopp. The agency stated that based on the knowledge it had gained from the documents and the expert group report, the privacy violations were too severe for the app to be allowed to continue operating (DPA, 2020e). It also agreed to NIPH's request for a meeting, but made clear that all input to the case needed to be provided in writing. This shows how the DPA wanted to keep any subsequent interaction between regulator and regulated entities at a formal level.

NIPH stopped its work with personal data on June 16, and at this point Smittestopp 1 was rated by Amnesty International as one of the most intrusive apps in the world (Amnesty International, 2020), intensifying the public shaming already started by the DPA. The DPA permanently banned the use of Smittestopp 1 on July 6. In its official ban letter to NIPH, the DPA further specified that any activity from then on would be closely monitored and controlled (DPA, 2020f).

4.5 | Phase 4: Smittestopp 2

After the ban, NIPH was still committed to aiding manual infection tracking in Norway through the use of technology. It began reworking the app in September 2020, with assistance from the private firm Netcompany (NIPH, 2020b). This time, the development of the app was approached completely differently. Many lessons were learned during development of the first app. Technology and privacy experts were included in development, and the DPA was continually updated and consulted throughout the process (Interviewees 6, 14). Nevertheless, the DPA reminded NIPH that it was closely monitoring the new app and that it had the authority to demand and obtain all relevant information for inspection (DPA, 2020g).

Technically, the new app included only Bluetooth and not GPS and made use of decentralized data storage. It was also based on open source, ensuring the needed transparency (NIPH, 2020b). Furthermore, NIPH spent more time attending to the technicalities and privacy issues that had been criticized previously (Interviewees 12, 15). Regarding context, uncertainty was lower at this time, and the government had more knowledge about the crisis (Kvinnsland et al., 2021). NIPH had also learned more about how to interpret the law from the DPA. In an interview, the head of the DPA stated that the DPA had told NIPH what type of information it had to provide to citizens downloading the app (Interviewee 6).

In December 2020, the DPA said that the new app was more privacy friendly and praised NIPH for its "good assessments" (DPA, 2020h). It added that it could not guarantee that it would not intervene once more, as this was complicated technology. On December 21, 2020, the app was launched. As of September 2021, it is still in use and the DPA has not intervened since, implying its approval.

5 | DISCUSSION AND CONCLUSION

The theoretical section of this article proposed three different types of regulatory intervention—rule-based, idea-based, and norm-based—for regulating emerging technology in times of crisis. All three approaches display quite different perspectives on regulation, each with their strengths and weaknesses. It was suggested that different levels of uncertainty, time pressure, and regulator's experience with regulatees' responses would impact which type of regulatory intervention regulators would be likely to embrace. Given these analytical directions, the following discussion summarizes the empirical findings and seeks to understand the various regulatory interventions chosen by the DPA when regulating Smittestopp. Building on this discussion, implications for further research are considered.

As the analysis reveals, determining regulatory intervention during the COVID-19 crisis was not an easy task for the Norwegian DPA. The data show that the DPA changed its approaches throughout the crisis, primarily based on knowledge of the technology and of the activities of regulatees, as well as its own experience with regulation and regulatees' responses to this regulation. Table 3 provides an overview of the uncertainty and urgency of the crisis, as well as the DPA's interventions.

In the beginning of the crisis, the DPA consistently conveyed an openness to new solutions and stated that privacy laws were not necessarily a hindrance to technological development. The work by the DPA was primarily communicative and idea-based, taking the form of either

TABLE 3 Timeline of regulatory interventions during the COVID-19 crisis

Regulation phase	Empirical evidence	Regulatory intervention	Uncertainty	Urgency
First phase: March 12–April 26, 2020	DPA converses with NIPH/Simula, emphasizing voluntariness, transparency, democracy, privacy-by-design, and open-source code.	Idea-based intervention.	High uncertainty (scarce information about the app and the virus).	High urgency (critical demand for information for the DPA on how to regulate such technology).
Second phase: April 27–June 11, 2020	DPA undertakes: (1) Inspection, auditing of technology. (2) Public shaming through media, stating rationale for rules.	Rule-based (and partly norm-based) intervention.	High uncertainty (still scarce information about the app and the virus; DPA does not know what NIPH/Simula are up to).	High urgency (DPA realizing that regulated entities did not change their behavior).
Third phase: June 12–October 5, 2020	DPA bans technology and ensures future control.	Rule-based intervention.	Medium uncertainty (enough information for the DPA to ban the app, in its opinion).	Medium urgency (NIPH stops its work on personal data).
Fourth phase: October 6–December 21, 2020	DPA investigates and controls new technology. Also praises NIPH for its work. DPA approves technology.	Rule-based and norm-based interventions.	Medium/low uncertainty (DPA knows what the technology does and is involved in the process. Government knows more about the virus).	Low urgency (DPA has control and adequate information about the app).

direct dialogue with the regulated entities (NIPH and Simula) or updates to its website and media. NIPH and Simula appeared to perceive the rules as ambiguous, creating an opportunity for the DPA to provide its interpretation of privacy rules. As shown in Table 3, the DPA was generic about what fundamental beliefs should underlie the technology—for example, transparency—and specific when it came to the measures within the technology—for example, privacy-by-design—both of which are examples of idea-based regulation. This initial communication focus is consistent with findings in a recent study of crisis management in Norway, where the government at large focused on creating a fundamental common objective for combating the coronavirus crisis by shaping shared understandings of what the crisis was about and how society must deal with it (Christensen & Lægreid, 2020).

Lack of information about the contact tracing app and lack of response from regulatees was what prompted a change in regulatory intervention, causing the shift to the second regulation phase. This happened about six weeks after the initial announcement of the app (see Table 3). During this phase, the DPA formally inspected NIPH and Simula in order to retrieve information with the goal of reducing uncertainty about the technology. Throughout this stage, the DPA also repeatedly stated the reasons for inspection and the rationales for relevant laws, whether on its website, in Norwegian media, or to NIPH directly; these repeated statements can be regarded at least in part as a form of public shaming. Hence, here we see a predominantly rule-based approach (inspection) with certain facets of a norm-based appeal (naming and shaming).

Based on the regulatees' response to the regulation, the DPA again saw no other option but to alter its approach once more, moving to a third phase of regulation. At this stage, however, while the parameters of the crisis were still uncertain, uncertainty about the technology had been reduced as the DPA now had clear knowledge about what technological and privacy measures the regulatees had and had not implemented. With increased certainty, the DPA expanded its formal efforts by banning Smittestopp 1 and ensuring that it maintained future control of app development. The regulation at this stage was thus solely rule-based. With the introduction of Smittestopp 2 in phase four, the DPA remained in control but also praised the work of NIPH.

Consequently, the preceding elaborations suggest that regulatory interventions on the part of DPA depended on the level of uncertainty with respect to the crisis (due to the virus itself and the effects of lockdowns) and the contact-tracing technology, and how these evolved over time. To sum up, at the outset of the crisis, the DPA completely followed an idea-based approach. In phase two, rule- and norm-based interventions were embraced. Thereafter, the DPA pursued a strictly rule-based approach with the ban of the contact-tracing app. Finally, after the creation of Smittestopp 2, the DPA controlled the technology with a rule-based intervention but supported the intervention with norm-based elements.

Some propositions may be formulated based on the analysis above regarding the study of other types of (emerging) technologies in extreme situations and the study of regulation in crisis situations more generally. One can expect to see idea-based interventions at the start of a crisis, because regulators are likely to keep an open mind regarding ways to combat it. At this point, there is expected to be a mixture of perceived ambiguous application of rules, uncertainty regarding the nature of the crisis and the emerging technology, and the need to facilitate technological development to combat the crisis. This in turn creates an opportunity for regulators to communicate their own ideas about and interpretations of rules and technology and what values are important in crisis situations. Regulators might do this in order to attempt to reduce uncertainty, but also to impose their own ideas in order to impact the cognitive structures and beliefs of regulatees within the relevant regulatory field (Black, 2002).

Subsequent regulation in crisis situations will depend on whether regulatees are responsive to the initial interventions by the regulator, and whether uncertainty is reduced. On the one hand, one can expect that if regulators are successful in their interventions, they will want to

avoid an adversarial relationship and will support the work of regulatees using norm-based measures such as praising. On the other hand, one can expect that if uncertainty is not reduced and regulatees are non-responsive, regulators will instead embrace rule-based measures such as investigations in order to confrontationally force a reduction of uncertainty regarding technology, likely in combination with norm-based shaming.

Even further into the crisis, there is a presumed increase of knowledge among government officials, the public, and relevant actors about the extreme situation and its impact on society. Additionally, interactions with regulatees provide the regulator with knowledge about the technology and about regulatees' behavior. Thus, on the one hand, one can postulate that a rule-based intervention will intensify by shifting to the use of sanctions, control, and command (as opposed relying on investigations) in situations in which time pressure increases and regulatees have not responded to either initial or subsequent interventions. On the other hand, if norm-based interventions have in fact been previously successful in reducing technological uncertainty earlier in the crisis, it is also likely that regulators will continue to pursue norm-based interventions in order to avoid an adversarial approach. This may occur in conjunction with formal incentives associated with a rule-based intervention. Idea-based interventions are highly unlikely at this point simply because time pressure is too great for this approach to have a significant impact.

Overall, idea-based regulation emerges as an opportunity for regulators to structure beliefs and ideas regarding technology when knowledge is limited, uncertainty is high, and time is pressing, as well as when other measures run the risk of curbing the necessary development of technology. Norm-based and rule-based intervention in various forms are more likely to appear as a crisis develops and uncertainty is reduced.

At a general level, this study contributes to deepening our understanding of the hitherto underexplored phenomenon of regulating emerging technology in crisis. Its findings demonstrate that we need to understand the exercise of different regulatory interventions based on levels of uncertainty and urgency. Moreover, the study suggests that idea-based regulation through regulatory conversations and communication is a key site of analysis when seeking to understand regulation in the context of crisis and emerging technology.

The suggested propositions can be tested on other digital tools developed during the COVID-19 pandemic. These tools involve big data, artificial intelligence, deep learning models, 5G technology, geospatial technology, robotics, smart applications, telemedicine, blockchain, and the Internet of Things (Mbunge et al., 2021). Such technologies present puzzles for regulators for both the present and the future. These technologies can also emerge in sectors such as finance, climate, or energy. Other types of technologies, like military technology, nanotechnology, or vaccines, are likewise often developed under conditions of great uncertainty in response to crisis. These technologies develop quickly, and often have unclear implications in both legal and moral terms (Mandel, 2009), which requires an intricate understanding of how they are regulated.

This study has several limitations. First, the propositions presented here are specifically related to crisis situations, which means that in more ordinary or stable circumstances they may not have the same applicability. Nevertheless, idea-based regulation is available outside of crises, although its effects may be uncertain and its outcomes are likely to be contested (Gilad, 2014).

Second, this study of how the dynamics of the three regulatory interventions can unfold must be considered in light of the political and administrative-legal domain in which they occurred. Norway is a country where the regulatory capacity of agencies is generally high. In this article's empirical case, the regulator has the final word, meaning the regulator can weigh its options and ultimately choose to sanction a technology that could potentially be vital in combating the pandemic. Not all regulators have such capacities, and this study may thus be more relevant for countries and policy sectors with more powerful regulators.

Additionally, this study concerns a case of "regulation inside government" (Hood et al., 1999), where one government body regulates another. Under the GDPR framework in Europe, and in the case of DPAs in Europe, it is reasonable to assume that this would be the case for private actors as well. However, whether this is the case under different privacy laws and with different regulatory agencies is an empirical question that future research should seek to answer.

Moreover, the COVID-19 pandemic spans a relatively long period of time, which may suggest that the dynamics among regulatory interventions observed in this study could be different in crises with shorter timescales. Relatedly, the COVID-19 pandemic is not the first crisis in which government and regulators have needed to balance privacy, individual freedom, and surveillance. For instance, there have been health crises in the past where the relevance of epidemiological, technological, or governmental surveillance has been emphasized. Two examples are the 1957–1958 global influenza pandemic (Flahault & Zylberman, 2010) and the 2009 global swine flu pandemic (Baekkeskov, 2016). In both cases, governments across the globe had to monitor and contain a virus in order to avoid (extremely) high infection rates and to eventually facilitate vaccination.

Future research may take inspiration from the study at hand and investigate regulation in previous health crises, or regulation of other types of technology, in order to observe changes over time and to observe changes over time from a global perspective and make comparisons. Overall, the analytical directions and empirical findings of this study can guide researchers in their study of future events as well as of past crises, allowing us to gain a more informed understanding of regulatory dynamics in crisis situations.

ACKNOWLEDGMENTS

The author would like to thank Tobias Bach and Tom Christensen as well as the anonymous reviewers for their helpful comments. The author would also like to thank participants at the December 2020 ECPR RegGov ECN conference and the December 2020 PBO research group seminar at the Department of Political Science, University of Oslo, for comments on earlier drafts.

ORCID

Jonas Lund-Tønnesen https://orcid.org/0000-0002-4544-7266

REFERENCES

Abbot, Carolyn. 2012. "Bridging the Gap—Non-state Actors and the Challenges of Regulating New Technology." *Journal of Law and Society* 39(3): 329–58. https://doi.org/10.1111/j.1467-6478.2012.00588.x.

Akinsanmi, Titi, and Aishat Salami. 2021. "Evaluating the Trade-Off between Privacy, Public Health Safety, and Digital Security in a Pandemic." *Data & Policy* 3: e27.

Ali, Christopher, and Manuel Puppis. 2018. "When the Watchdog Neither Barks Nor Bites: Communication as a Power Resource in Media Policy and Regulation." *Communication Theory* 28(3): 270–91. https://doi.org/10.1093/ct/qtx003.

Almeida, Rita, and Pedro Carneiro. 2012. "Enforcement of Labor Regulation and Informality." *American Economic Journal: Applied Economics* 4(3): 64–89. https://doi.org/10.1257/app.4.3.64.

Amnesty International. 2020. "Bahrain, Kuwait og Norge har de verste korona-appene." https://amnesty.no/bahrain-kuwait-og-norge-har-de-verste-korona-appene.

Ansell, Chris, Arjen Boin, and Ann Keller. 2010. "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System." *Journal of Contingencies and Crisis Management* 18(4): 195–207. https://doi.org/10.1111/j.1468-5973.2010.00620.x.

Archibugi, Daniele, Andrea Filippetti, and Marion Frenz. 2013. "Economic Crisis and Innovation: Is Destruction Prevailing over Accumulation?" *Research Policy* 42(2): 303–14. https://doi.org/10.1016/j.respol.2012.07.002.

Ayres, Ian, and John Braithwaite. 1992. *Responsive Regulation, Transcending the Deregulation Debate*. Oxford: Oxford University Press.

Bach, Tobias, Marlene Jugl, Dustin Köhler, and Kai Wegrich. 2021. "Regulatory Agencies, Reputational Threats, and Communicative Responses." *Regulation & Governance*. https://doi.org/10.1111/rego.12421

Baekkeskov, Erik. 2016. "Same Threat, Different Responses: Experts Steering Politicians and Stakeholders in 2009 H1N1 Vaccination Policy-Making." *Public Administration* 94(2): 299–315.
Baldwin, Robert. 1997. "Regulation: After Command and Control." In *The Human Face of Law*, edited by Keith Hawkins, 65–84. Oxford: Oxford University Press.
Baldwin, Robert, and Julia Black. 2008. "Really Responsive Regulation." *Modern Law Review* 71(1): 59–94. https://doi.org/10.1111/j.1468-2230.2008.00681.x.
Bardach, Eugene, and Robert A. Kagan. 2017. *Going by the Book: The Problem of Regulatory Unreasonableness*. London: Routledge.
Barley, Stephen R., and Pamela S. Tolbert. 1997. "Institutionalization and Structuration: Studying the Links between Action and Institution." *Organization Studies* 18(1): 93–117.
Bennett, Colin J., and Charles D. Raab. 2020. "Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective." *Regulation & Governance* 14(3): 447–64.
Black, Julia. 2002. "Regulatory Conversations." *Journal of Law and Society* 29(1): 163–96. https://doi.org/10.1111/1467-6478.00215.
Black, Julia. 2010. "The Role of Risk in Regulatory Processes." In *The Oxford Handbook of Regulation*, edited by Robert Baldwin, Martin Cave, and Martin Lodge. Oxford: Oxford University Press.
Black, Julia, and Robert Baldwin. 2010. "Really Responsive Risk-Based Regulation." *Law & Policy* 32(2): 181–213. https://doi.org/10.1111/j.1467-9930.2010.00318.x.
Boin, Arjen, Paul't Hart, and Allan McConnell. 2009. "Crisis Exploitation: Political and Policy Impacts of Framing Contests." *Journal of European Public Policy* 16(1): 81–106. https://doi.org/10.1080/13501760802453221.
Boin, Arjen, Paul't Hart, Eric Stern, and Bengt Sundelius. 2005. *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge: Cambridge University Press.
Boustead, Anne E. 2021. "Privacy Protections and Law Enforcement Use of Prescription Drug Monitoring Databases." *Law & Policy* 43(3): 229–61.
Braithwaite, J. 2017. "Types of Responsiveness." In *Regulatory Theory: Foundations and Applications*, edited by Peter Drahos. Canberra: ANU Press.
Budd, Jobie, Benjamin S. Miller, Erin M. Manning, Vasileios Lampos, Mengdie Zhuang, Michael Edelstein, and Geraint Rees. 2020. "Digital Technologies in the Public-Health Response to COVID-19." *Nature Medicine* 26(8): 1183–92. https://doi.org/10.1038/s41591-020-1011-4.
Burby, Raymond J., and Robert G. Paterson. 1993. "Improving Compliance with State Environmental Regulations." *Journal of Policy Analysis and Management* 12(4): 753–72. https://doi.org/10.2307/3325349.
Christensen, Tom, and Per Lægreid. 2020. "Balancing Governance Capacity and Legitimacy: How the Norwegian Government Handled the COVID-19 Crisis as a High Performer." *Public Administration Review* 80(5): 774–9. https://doi.org/10.1111/puar.13241.
Christensen, Tom, Per Lægreid, and Lise H. Rykkja. 2016. "Organizing for Crisis Management: Building Governance Capacity and Legitimacy." *Public Administration Review* 76(6): 887–97. https://doi.org/10.1111/puar.12558.
Coglianese, Cary, J. Nash, and Todd Olmstead. 2003. "Performance-Based Regulation Prospects and Limitations in Health, Safety and Environmental Protection." *Administrative Law Revview* 55: 705–29.
Cornelissen, Joep P., Rodolphe Durand, Peer C. Fiss, John C. Lammers, and Eero Vaara. 2015. "Putting Communication Front and Center in Institutional Theory and Analysis." *The Academy of Management Review* 40(1): 10–27. https://doi.org/10.5465/amr.2014.0381.
Corona Commission. 2021. "Referater fra intervjuer i forbindelse med NOU 2021:6." https://www.koronakommisjonen.no/dokumenter/.
DiMaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2): 147–60.
DPA. 2020a. "Ny sporings-app for å hindre koronasmitte." https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-sporings-app-for-a-hindre-koronasmitte/.
DPA. 2020b. "Starter kontroll av FHIs Smittestopp-app." https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp/.
DPA. 2020c. "Personvernpodden." https://www.datatilsynet.no/regelverk-og-verktoy/personvernpodden/.
DPA. 2020d. "Krav om redegjørelse – appen Smittestopp." https://www.datatilsynet.no/contentassets/22b1296d0ab645609d3c040e9822e8d9/20-01170-8-krav-om-redegjorelse.pdf.
DPA. 2020e. "Varsel om vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp." https://www.datatilsynet.no/contentassets/1c72ac62cac145efa242942ca34c2cd0/20-02058-9-varsel-om-vedtak-om-midlertidig-forbud-mot-a-behandle-personopplysninger—smittestopp.pdf.
DPA. 2020f. "Vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp." https://www.fhi.no/contentassets/b62750459eeb4bf6ac2fe7d32ad44206/~-20_02058-15-vedtak-om-midlertidig-forbud-mot-a-behandle-personopplysninger.pdf.
DPA. 2020g. "Tilbakemelding vedrørende videre saksgang." https://www.fhi.no/contentassets/93841455d6554ccb869f3a2fe362b9f6/vedlegg/motereferater/~-20_11308-18-20_02058-20tilbakemelding-vedrorende-videre-saksgang-510802_1_1.pdf.

DPA. 2020h. "Ny Smittestopp lansert." https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-smittestopp-lansert/.
Expert-Group. 2020a. "Foreløpig rapport for kodegjennomgang av løsning for digital smittesporing av koronaviruset." Norwegian Government. https://www.regjeringen.no/globalassets/departementene/hod/fellesdok/rapporter/200409_forelppig_rapport_ekspertgruppe_sporingsapp.pdf.
Expert-Group. 2020b. "Endelig rapport for kildegjennomgang av løsning for digital smittesporing av koronaviruset." Norwegian Government. https://www.regjeringen.no/contentassets/88ec3360adae44a1a9635fd6c1a58fca/200520_rapport_ekspertgruppa_smittestopp.pdf.
Fairman, Robyn, and Charlotte Yapp. 2005. "Enforced Self-Regulation, Prescription, and Conceptions of Compliance within Small Businesses: The Impact of Enforcement." *Law & Policy* 27(4): 491–519. https://doi.org/10.1111/j.1467-9930.2005.00209.x.
Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing." *Science* 368(6491): eabb6936. https://doi.org/10.1126/science.abb6936.
Fitzgerald, Brian. 2006. "The Transformation of Open Source Software." *MIS Quarterly* 30: 587–98.
Flahault, Antoine, and Patrick Zylberman. 2010. "Influenza Pandemics: Past, Present and Future Challenges." *Public Health Reviews* 32(1): 319–40.
Fligstein, Neil. 2001. "Institutional Entrepreneurs and Cultural Frames: The Case of the European Union's Single Market Program." *European Societies* 3(3): 261–87. https://doi.org/10.1080/14616690120079332.
Fortin, Neal D. 2016. *Food Regulation: Law, Science, Policy, and Practice*. Hoboken, NJ: Wiley.
Gasser, Urs, Marcello Ienca, James Scheibner, Joanna Sleigh, and Effy Vayena. 2020. "Digital Tools against COVID-19: Taxonomy, Ethical challenges, and Navigation Aid." *Lancet Digital Health* 2(8): e425–34. https://doi.org/10.1016/S2589-7500(20)30137-0.
Gezelius, Stig S., and Maria Hauck. 2011. "Toward a Theory of Compliance in State-Regulated Livelihoods: A Comparative Study of Compliance Motivations in Developed and Developing World Fisheries." *Law & Society Review* 45(2): 435–70.
Gilad, Sharon. 2014. "Beyond Endogeneity: How Firms and Regulators Co-construct the Meaning of Regulation." *Law & Policy* 36(2): 134–64.
Goffman, Erving. 1974. *Frame Analysis*. Cambridge: Harvard University Press.
Gray, Wayne B., and Mary E. Deily. 1996. "Compliance and Enforcement: Air Pollution Regulation in the U.S. Steel Industry." *Journal of Environmental Economics and Management* 31(1): 96–111. https://doi.org/10.1006/jeem.1996.0034.
Grekousis, George, and Ye Liu. 2021. "Digital Contact Tracing, Community Uptake, and Proximity Awareness Technology to Fight COVID-19: A Systematic Review." *Sustainable Cities and Society* 71: 102995. https://doi.org/10.1016/j.scs.2021.102995.
Gunningham, Neil, Peter N. Grabosky, and Darren Sinclair, eds. 1998. *Smart Regulation: Designing Environmental Policy (Oxford Socio-Legal Studies)*. Oxford: Clarendon Press.
Gunningham, Neil, and Robert A. Kagan. 2005. "Regulation and Business Behavior." *Law & Policy* 27(2): 213–8. https://doi.org/10.1111/j.1467-9930.2005.00197.x.
Hagemann, Ryan, Jennifer Huddleston Skees, and Adam Thierer. 2018. "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future." *Colorado Technology Law Journal* 17: 37.
Hatch, Mary Jo, and Sanford B. Erhlich. 1993. "Spontaneous Humour as an Indicator of Paradox and Ambiguity in Organizations." *Organization Studies* 14(4): 505–26. https://doi.org/10.1177/017084069301400403.
Hood, Christopher, Oliver James, George Jones, Colin Scott, and Tony Travers. 1999. *Regulation inside Government: Waste-Watchers, Quality Police, and Sleazebusters*. Oxford: Oxford University Press.
Kagan, Robert A., and John T. Scholz. 1984. "The Criminology of the Corporation and Regulatory Enforcement Strategies." In *Enforcing Regulation*, edited by Keith Hawkins and John M. Thomas. Boston: Kluwer-Nijhoff.
Knight, Frank H. 1921. *Risk, Uncertainty and Profit*, Vol 31. Boston: Houghton Mifflin.
Kvinnsland, Stener, Astri Aas-Hansen, Geir Sverre Braut, Knut Eirik Dybdal, Tone Fløtten, Rune Jakobsen, Toril Johansson, et al. 2021. "Myndighetenes Håndtering av Koronapandemien." Rapport fra Koronakommisjonen. Oslo: Prime Minister's Office. NOU 2021: 6. https://www.regjeringen.no/contentassets/5d388acc92064389b2a4e1a449c5865e/no/pdfs/nou202120210006000dddpdfs.pdf.
Lewallen, Jonathan. 2020. "Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity." *Regulation & Governance* 15(4): 1035–52. https://doi.org/10.1111/rego.12341.
Lodge, Martin, and Kai Wegrich. 2012. *Managing Regulation: Regulatory Analysis, Politics and Policy*. Basingstoke: Palgrave Macmillan.
Mandel, Gregory N. 2009. "Regulating Emerging Technologies." *Law, Innovation and Technology* 1(1): 75–92. https://doi.org/10.1080/17579961.2009.11428365.
Mbunge, Elliot, Boluwaji Akinnuwesi, Stephen G. Fashoto, Andile S. Metfula, and Petros Mashwama. 2021. "A Critical Review of Emerging Technologies for Tackling COVID-19 Pandemic." *Human Behavior and Emerging Technologies* 3(1): 25–39. https://doi.org/10.1002/hbe2.237.

Meijer, Albert Jacob, Miriam Lips, and Kaiping Chen. 2019. "Open Governance of Cities: A New Paradigm for Understanding Urban Collaboration." *Frontiers in Sustainable Cities* 1: 3. https://doi.org/10.3389/frsc.2019.00003.
Morley, Jessica, Josh Cowls, Mariarosaria Taddeo, and Luciano Floridi. 2020. "Ethical Guidelines for COVID-19 Tracing Apps." *Nature* 582(7810): 29–31. https://doi.org/10.1038/d41586-020-01578-0.
NBT. 2020. "Digital Smittesporing." The Norwegian Board of Technology. https://teknologiradet.no/event/digital-smittesporing-og-personvern/.
NIPH. 2020a. "Smittestopp – ny app fra Folkehelseinstituttet." Norwegian Institute for Public Health. https://www.fhi.no/nyheter/2020/ny-app-fra-folkehelseinstituttet/.
NIPH. 2020b. "Oppdateringer om arbeidet med nye Smittestopp." Norwegian Institute for Public Health. https://www.fhi.no/om/smittestopp/digital_smittesporing/.
NRK. 2020a. "Nesten 1,5 millioner nedlastninger." https://www.nrk.no/nyheter/nesten-1_5-millioner-nedlastinger-1.14997489.
NRK. 2020b. "Smittestopp-app får varsel om pålegg." https://www.nrk.no/norge/smittestopp-app-far-varsel-om-palegg-1.15014601.
Perrow, Charles. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.
Personal Data Act, 2018. "Lov 15. juni 2018 nr. 38 om behandling av personopplysninger."
Phillips, Nelson, Thomas B. Lawrence, and Cynthia Hardy. 2004. "Discourse and Institutions." *The Academy of Management Review* 29(4): 635–52. https://doi.org/10.2307/20159075.
Picciotto, Sol. 2007. "Constructing Compliance: Game Playing, Tax Law, and the Regulatory State." *Law & Policy* 29(1): 11–30. https://doi.org/10.1111/j.1467-9930.2007.00243.x.
Picciotto, Sol. 2015. "Indeterminacy, Complexity, Technocracy and the Reform of International Corporate Taxation." *Social & Legal Studies* 24(2): 165–84. https://doi.org/10.1177/0964663915572942.
PrivacyRules. 2020. "PrivacyRules Webinar on Tracing Apps." https://www.privacyrules.com/privacy-global-expertise/privacyrules-webinar-tracing-apps-0006979.html.
RDI. 2020. "Forskrift om Digital Smittesporing og Epidemikontroll i Anledning Utbrudd av COVID-19." https://lovdata.no/dokument/LTI/forskrift/2020-03-27-475.
Rorie, Melissa L., Sally S. Simpson, Mark A. Cohen, and Michael P. Vandenbergh. 2018. "Examining Procedural Justice and Legitimacy in Corporate Offending and Beyond-Compliance Behavior: The Efficacy of Direct and Indirect Regulatory Interactions." *Law & Policy* 40(2): 172–95.
Rosenthal, Uriel, Michael T. Charles, and Paul t' Hart. 1989. *Coping With Crises: The Management of Disasters, Riots and Terrorism*. Springfield, IL: C.C. Thomas Publishers.
Rotolo, Daniele, Diana Hicks, and Ben R. Martin. 2015. "What Is an Emerging Technology?" *Research Policy* 44(10): 1827–43. https://doi.org/10.1016/j.respol.2015.06.006.
Schumpeter, Joseph A. 1934. *The Theory of Economic Development*. Cambridge: Harvard University Press.
Schwartz, Richard D., and Sonya Orleans. 1967. "On Legal Sanctions." *The University of Chicago Law Review* 34(2): 274–300. https://doi.org/10.2307/1598934.
Scott, W. Richard. 2003. "Institutional Carriers Reviewing Modes of Transporting Ideas over Time and Space and Considering their Consequences." *Industrial and Corporate Change* 12(4): 879–94. https://doi.org/10.1093/icc/12.4.879.
Scott, W. Richard. 2008. "Lords of the Dance: Professionals as Institutional Agents." *Organization Studies* 29(2): 219–38. https://doi.org/10.1177/0170840607088151.
Scott, W. Richard. 2014. *Institutions and Organizations: Ideas, Interests, and Identities*, 4th ed. Thousand Oaks, CA: Sage.
Sechser, Todd S., Neil Narang, and Caitlin Talmadge. 2019. "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War." *Journal of Strategic Studies* 42(6): 727–35. https://doi.org/10.1080/01402390.2019.1626725.
Simula. 2020a. "Smittestopp og erfaringer fra digital smittesporing." https://www.simula.no/news/smittestopp-og-erfaringer-fra-digital-smittesporing.
Simula. 2020b. "Sammenligning av alternative løsninger for digital smittesporing." https://www.simula.no/sites/default/files/sammenligning_alternative_digital_smittesporing.pdf.
Talmadge, Caitlin. 2019. "Emerging Technology and Intra-war Escalation Risks: Evidence from the Cold War, Implications for Today." *Journal of Strategic Studies* 42(6): 864–87. https://doi.org/10.1080/01402390.2019.1631811.
Tekna. 2020. "Teknologi og rettsstatsprinsipper i krisetider." https://www.tekna.no/fag-og-nettverk/IKT/ikt-bloggen/teknologi-i-krisetider/.
Thiemann, Matthias, and Jan Lepoutre. 2017. "Stitched on the Edge: Rule Evasion, Embedded Regulators, and the Evolution of Markets." *American Journal of Sociology* 122(6): 1775–821. https://doi.org/10.1086/691348.
Tyler, Tom R. 2021. *Why People Obey the Law*. Princeton: Princeton University Press.
Whitelaw, Sera, Mamas A. Mamas, Eric Topol, and Harriette G. C. Van Spall. 2020. "Applications of Digital Technology in COVID-19 Pandemic Planning and Response." *Lancet Digital Health* 2(8): e435–40. https://doi.org/10.1016/S2589-7500(20)30142-4.
Winter, Soren C., and Peter J. May. 2001. "Motivation for Compliance with Environmental Regulations." *Journal of Policy Analysis & Management* 20(4): 675–98. https://doi.org/10.2307/3325778.

Yin, Robert K. 2014. *Case Study Research: Design and Methods*, 5th ed. Los Angeles: SAGE.

AUTHOR BIOGRAPHY

Jonas Lund-Tønnesen is a Doctoral Research Fellow the Department of Political Science, University of Oslo, Norway. His research interests include digital technology, governance, regulation, and crisis management.

How to cite this article: Lund-Tønnesen, Jonas. 2022. "Regulating Emerging Technology in Times of Crisis: Digital Contact Tracing in Norway during the COVID-19 Pandemic." *Law & Policy* 44(3): 278–298. https://doi.org/10.1111/lapo.12195

APPENDIX A: OVERVIEW OF DATA SOURCES

Time period	Data sources
Smittestopp 1 (March–July 2020)	**DPA and NIPH documents:** DPA (2020a, 2020b, 2020d, 2020e, 2020f), NIPH (2020a, 2020b) **Laws:** RDI (2020), Personal Data Act (2018) **Expert-Group reports:** Expert-Group (2020a, 2020b) **Conference/debate:** Tekna (2020), NBT (2020) **Podcast:** From May/July 2002, DPA (2020c) **Media:** NRK (2020a, 2020b)
Post-ban and Smittestopp 2 (July 2020–January 2021).	**DPA and NIPH documents:** DPA (2020g, 2020h), NIPH (2020b) **Commission evaluation:** Kvinnsland et al. (2021). **Evaluation report:** Simula (2020b) **Interviews:** 16 interviews with DPA, NIPH, and Simula +32 interviews with ministers and top administrative leaders (Corona Commission, 2021) **Conference/Debate:** PrivacyRules (2020), Simula (2020a) **Podcast:** From October/December, DPA (2020c)

Article 2: The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic

Publication status: Published in *International Public Management Journal*, 2023, *26*(1), 126-144.

INTERNATIONAL PUBLIC MANAGEMENT JOURNAL
2023, VOL. 26, NO. 1, 126–144
https://doi.org/10.1080/10967494.2022.2112328

The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic

Jonas Lund-Tønnesen and Tom Christensen

University of Oslo

ABSTRACT

Input, throughput, and output legitimacy of government measures are considered to be essential for governance capacity in crisis. During the COVID-19 crisis, governments around the world developed digital contact-tracing applications to support their crisis management—with varying degrees of success. While Norway is seen as a high performer in the crisis, the contact-tracing app called Smittestopp developed in Norway had little impact. Using a case study, we studied the governance capacity and legitimacy of this technology in terms of how it was developed, how much it was utilized by citizens, and its usefulness relative to other government measures. Although the app did very little to help the COVID-19 crisis management in Norway, we identify some important lessons to be learned. We argue that the initial input and throughput legitimacy is important if a government policy is to maintain output legitimacy over time and be effective in a crisis. Consequently, this study contributes to the literature on governance capacity and legitimacy in crisis management.

ARTICLE HISTORY
Received 9 August 2021
Accepted 6 August 2022

Introduction

When a major crisis such as the COVID-19 pandemic strikes, the government response can be evaluated in terms of preparation, mitigation, sense-making, meaning-making, and learning (Boin et al. 2005). All these aspects or phases are related to the two central concepts in crisis management: governance capacity and governance legitimacy (Christensen, Laegreid, and Rykkja 2016). Governance capacity, alluding generally to a government's ability to organize and to the resources it has, will in a pandemic include the healthcare provision available, the level of training, intra- and intergovernmental structures, delegation of authority, specialized competences, etc. Lodge and Wegrich (2014) divide governance capacity into four categories—analytical, coordination, regulatory, and delivery capacity.

Governance legitimacy primarily deals with the relationship between government and citizens. How convincing is the government in meaning-making, i.e., in explaining to citizens what the crisis is about and how it plans to deal with it (Ansell, Boin, and Keller 2010)? How do citizens receive communications from the government, and how positive is their perception of how the government is coping with the crisis? Do they trust the government, overall or more specifically (Easton 1965)? Governance legitimacy can be divided into input, throughput and output legitimacy (Scharpf 1999; Schmidt 2013).

There is a dynamic relationship between governance capacity and legitimacy (Christensen et al. 2016). If governance capacity is high in all aspects, citizens are also likely to respond positively,

CONTACT Jonas Lund-Tønnesen jonas.lund-tonnesen@stv.uio.no Department of Political Science, University of Oslo, Moltke Moes vei 31, Oslo 0316, Norway.

leading to a high score on legitimacy. Conversely, if governance legitimacy is low for various reasons, this may undermine governance capacity; citizens support is crucial, both because regulatory measures will be followed more loyally and because they contribute to local service provision most if they support the government. Therefore, governance legitimacy is crucial for governance capacity.

Among the central tools for handling the pandemic, the combination of testing, tracing, quarantine, and isolation has been seen as the most effective (Kucharski et al. 2020). Among those tools, contact-tracing technology has been regarded as a success factor among well-performing countries such as China, South Korea and Taiwan, even though many concerns have been raised related to human rights and violation of privacy (Cheng et al. 2020; Kostka and Habich-Sobiegalla 2020; Ryan 2020). Governments around the world developed digital contact-tracing applications (apps) to support their crisis management (Ferretti et al. 2020). These apps were designed in different ways and enjoyed varying degrees of success and acceptance among citizens (Oliver et al. 2020; Grekousis and Liu 2021).

In Norway, the digital app Smittestopp ("infection stop" in Norwegian) was developed as a key part of the government's infection tracking strategy (Meijerink et al. 2021). Although the Norwegian government is seen as a high performer in managing the crisis compared with many other countries (Christensen and Laegreid 2020a), its digital contact-tracing measures have had quite a low impact. The first version of the contact-tracing app, Smittestopp 1, was created during spring 2020 and eventually deemed illegal in June/July by the Norwegian Data Protection Authority (DPA) on the grounds that it intruded excessively into people's privacy. For this reason, it was eventually scrapped.

A second version of the app, Smittestopp 2, was launched in December 2020. This time it complied with all the regulations and adhered to the highest privacy standards for such technology. Despite this, the Norwegian population has made only limited use of it. This study seeks to understand why this was the case, and why the technology did not have much impact. The use of apps in contact-tracing during the pandemic is at the core of the interface between government capacity—how the apps are developed and organized—and governance legitimacy—how are they perceived by citizens.

Accordingly, the research questions of this study are:

RQ1: What characterized the two processes of developing digital contact-tracing technology in Norwayduring the COVID-19 pandemic with regards to the dynamics of governance capacity and legitimacy?

RQ2: How can we understand the use of the contact-tracing technology in relation to the other measures to deal with the pandemic?

The remainder of the study is organized as follows. We start by presenting the theoretical foundation, defining the concepts of crisis management, governance capacity and governance legitimacy. The next section elaborates on the overall COVID-19 pandemic context. This is followed by a description of our methods. We then compare the processes of developing the two versions of the contact-tracing app and discuss this in the light of governance capacity and legitimacy. Thereafter, we discuss this in relation to other crisis measures, conclude with our main results and discuss the further implications of the study as well as limitations.

Theory

Crisis management

Crisis management can be defined as the process whereby public (and private) organizations deal with a crisis before, during, and after it has occurred (Boin et al. 2005). It involves being prepared

for a crisis, meaning having a contingency plan and the necessary equipment, which overall was a problem in many countries when COVID-19 struck. Crisis management also involves handling the crisis, meaning using the resources available or mobilizing more resources (Lodge and Wegrich 2014). After the crisis is over, it is important to use the experience gained from it to generate feedback and to improve the crisis management system, so that it is better equipped to deal with a new crisis. All these instrumental factors are central aspects of what is called governance capacity, which will be discussed in more detail below (Christensen et al. 2016).

However, crisis management is much more than the technical aspects. When a crisis happens, central actors must try to make sense of it for the public, but it must also be able to communicate its crisis management, otherwise it is difficult for people to know how to respond to the crisis. This sense-making process (Weick 1995) may be smooth and dominated by top executives with unambiguous means-end thinking, but it may also be characterized by a variety of interests, different perceptions of the potential consequences of choosing certain solutions and by negotiation processes that end in compromises.

Another important aspect is meaning-making. The government has to communicate what the crisis is all about externally and make sense of it for citizens (You and Ju 2019). This communication is context-based, in the sense that there are structural and temporal constraints, and it may be more or less professional. Improved reputation management in a crisis reflects such professionalization, where certain symbols are used in a systematic way (Waeraas and Maor 2014). The combined features of sense-making and meaning-making are seen as deeply related to governance legitimacy, as we will discuss below.

A growing part of modern crisis management involves the use of technology (Meijer, Lips, and Chen 2019). Technologies developed to assist combating a crisis often come about rapidly and are called emerging or disruptive technologies (Rotolo, Hicks, and Martin 2015; Taeihagh, Ramesh, and Howlett 2021). Emerging technologies can be characterized as having five key attributes: they are radically new, grow fast, spread coherently, have prominent impact, and have uncertain outcomes (Rotolo et al. 2015:1833–1839). During the Covid-19 pandemic emerging technologies involving artificial intelligence (AI), 5 G-enabled e-health solutions, robotics, Big Data, Internet of things, and digital contact-tracing were developed across the world (Mbunge et al. 2021). For our study, digital contact-tracing apps for mobile phones are most relevant. We will analyze the development and use of such a technology in Norway by applying the concepts of governance capacity and governance legitimacy.

Governance capacity and governance legitimacy

Governance capacity deals primarily with resources and organization, meaning formal structural design and crisis-related procedures of the government apparatus (Christensen et al. 2016). The government must decide how much resources to allocate to combat a crisis, relative to those allocated for other societal purposes, and how to distribute resources among different aspects of a crisis. For example, in the case of the COVID-19 pandemic: health, economic concerns and social aspects (Christensen and Laegreid 2020b). It must also decide how to organize the handling of the crisis. Should authority and power be concentrated centrally or delegated to lower levels? Which public body should be the lead agency? And how should the influence of political, administrative, and expert actors be balanced?

Lodge and Wegrich (2014) distinguish between four types of governance capacity. *Analytical capacity* is a rather basic category concerning means-end thinking - what to do and how to do it. Without the ability to analyze information and without evidence-based expert advice, the risks and vulnerabilities will increase. This alludes to what is called the scientization of public decision making, which has been seen as crucial during the pandemic (Marcussen 2010). *Coordination capacity* is about how to cope with public organizations pulling in different directions during

crises. The challenges of inter- or intra-organizational coordination, whether vertical or horizontal (Egeberg 2012), are especially important during crises that represent typical "wicked issues," meaning reaching across sectors, institutions and levels (Head and Alford 2015).

Regulatory capacity deals with control, surveillance, oversight, and auditing, and is hence tightly connected to coordination capacity, since regulatory measures imply coordination both inside the public apparatus and vis-à-vis societal stakeholders and regulatees (Alemanno 2020). It presupposes that the legal preconditions are in place and that the government is not overstepping its authority. *Delivery capacity* is about providing public services during a crisis, which in particular connects with coordination capacity, i.e., are services available and in what ways (Gai and Tobe 2020). Providing services means both crisis- and non-crisis-related services. Many governments have, for example, been criticized for disregarding regular medical activities, such as cancer treatment and heart surgery, because nearly all the capacity of some hospitals has been directed toward treating COVID-19 patients.

In what ways are the different types of governance capacity relevant for understanding the development and use of a contact-tracing app? Generally, governance capacity is required in order to have the resources and organizational structure to develop such an app. More specifically, it takes analytical capacity, either in the public apparatus or in collaboration with the private sector, technically to develop an app. Coordination capacity may deal with bringing together this competence and making it work in practice. Regulatory capacity is necessary regarding the legal aspects of an app, ensuring that public authorities do not violate privacy and handle personal information appropriately. Delivery capacity deals potentially with making the app available and easy to use.

Governance legitimacy is about how the attitudes and actions of a government are received by citizens (Christensen et al. 2016). Trust and legitimacy are closely connected. Following Easton (1965), one can say that trust is either general/diffuse or specific. This can mean that citizens trust the government generally, in most respects, or they trust specific institutions or particular leaders in certain situations. High legitimacy may work well in crisis situations, because it represents what in organization theory is called slack (Cyert and March 1963), i.e., a situation where the government has reserves because demands are lower than resources. People may thus accept the government's actions and make them easier to implement and more effective.

Input legitimacy, throughput legitimacy, and *output legitimacy* are three types of governance legitimacy (Scharpf 1999; Schmidt 2013). *Input legitimacy* deals with how peoples' assessment and acceptance of the actions of leaders in crises are related to how compatible they think policies of government are with their own views. Participatory quality is, however, also important (Thiele and Pruin 2021). This refers to whether citizens feel involved in policymaking and policy implementation. A common problem for citizens in many countries during the pandemic has been that they have felt unable to participate in or influence government action. Government action and the motivations behind it has in many cases been rather paternalistic and hierarchical, asking people to be collectively oriented and disciplined to get through the crisis (Christensen and Laegreid 2020b). This has led to public debates and conflicts, both concerning the initial handling of the pandemic and the vaccine programs, but also related to the development and use of contact-tracing apps.

Throughput legitimacy deals with what goes on in the "black box," meaning in the governance apparatus; it is process-oriented and focuses on the quality of interactions (Schmidt 2013), which means the efficacy of all the different processes and the rules and procedures used in decision-making. It also deals with transparency and accountability, including ethical governance, but also inclusiveness and deliberative quality in interactions among governmental actors, as well as openness toward society.

Output legitimacy deals with the problem-solving quality of decisions, laws and rules, and measures such as contact-tracing apps, and has several institutional mechanisms connected with it. It deals with the extent to which government decisions, policies, means and measures resonate with the norms and values of citizens, and it contributes to identity-building and commitment (Cerutti and Lucarelli 2008).

There could be interesting dynamics among the three types of legitimacy. In the best of all worlds, input legitimacy will be high, in other words, processes will be inclusive and participative. This may then translate into high throughput legitimacy, meaning high quality internal processes, including openness to the public. This may in turn lead to high output legitimacy, meaning effective goal achievement and public acceptance of and support for government tools and performance. There could also, however, be less mutual reinforcement among the different types of legitimacy. Lack of participatory quality may carry over into skepticism about internal governmental processes and low legitimacy for performance and products.

In what way are these types of legitimacy relevant for discussing the development of a contact-tracing app? Input legitimacy may relate to whether citizens and civic groups affected by the policy or outside experts support the government or are participating in developing the app. Throughput legitimacy may deal with how well different governmental bodies or private firms participate in developing the app, while output legitimacy may relate to whether citizens trust the app and find it useful. Additionally, if the app undergoes different phases of development or is significantly changed in some way, there may be interaction between these phases, and between the different types of legitimacy in the phases.

Governance capacity and governance legitimacy, and the various aspects thereof, may be connected in different ways to developing a contact-tracing app. Analytical capacity may be an important precondition for overall high legitimacy through collaborating with private actors in the initial phase of input legitimacy, and for intra-governmental collaboration in the throughput legitimacy phase, not to mention for effectiveness and performance on the output legitimacy side. Coordination capacity may simply getting different public organizations to work constructively together to launch development with private providers, but also to balance and take into consideration various intra-governmental concerns in developing an app, which may increase the chances for its success, reflecting all the three types of legitimacy. From the input phase onwards, regulatory capacity may define the legal and other constraints for initiating an app and develop it further in the throughput phase, which may enhance its performance and output legitimacy. Delivery capacity may deal with working with the relevant stakeholders and the public in the input phase, coordinate different service-oriented needs among different public organizations in the throughput phase, and make the app user-friendly and available in the output phase, to increase the output legitimacy.

Although one might expect that an apparent improvement in government capacity would increase legitimacy, and specifically output legitimacy, this need not be the case, as would be a main thesis concerning the connection between Smittestopp 1 and 2. This dynamic must be seen in relation to the pandemic context and other government measures that deals with the crisis. One can expect that if other measures have been successful in the past, it is not all clear that citizens will think that the tracing technology is necessary when the Norwegian government (and society) had generally been seen as a high performer in the pandemic with its other measures (Christensen and Laegreid 2020a).

Generally, we would expect to see the dynamics between governance capacity and governance legitimacy to be reflected in how the Norwegian government worked with the contact-tracing app Smittestopp, and how the Norwegian people responded. The people's response can be seen in the number of downloads of Smittestopp 1 and Smittestopp 2, and in the number of reported infections in the apps in comparison to the number of infections in the country in general, reflecting output legitimacy.

Context

The central actors handling the pandemic in Norway has been the Prime Minister (PM), the Ministry of Health (MH), the Norwegian Directorate of Health (NDH) and the Norwegian Institute of Public Health (NIPH) (Askim and Bergström 2022). When COVID-19 broke out in China and later spread around the world, the NDH and NIPH urged the Norwegian government to stay calm and not to rush into imposing stringent regulations. This strategy seemed rational for some time but as the number of infections world-wide grew rapidly in late February and early March 2020, the government came under increasing pressure. Finally, it was decided on March 12. to "push the big button" and establish the most draconic regulatory measures since WW II. These measures, which never amounted to a real lock-down, consisted of advice on social distancing, sneezing, washing hands, etc., but also encompassed closing kindergartens, schools and universities and various kinds of businesses, stopping cultural and sports events, and restricting movement both into Norway from outside and internally (Christensen and Laegreid 2020a). In seeking to balance the main concerns, the government favored the precautionary principle and gave priority to health over economic and social considerations. Economic hardship caused by the restrictions was alleviated through various economic stimulus packages, reflecting the country's affluence, while social concerns remained in the background the whole time (Christensen and Laegreid 2020b).

In deciding on the regulatory measures, the government mainly took advice from the NDH, while the NIPH's line generally deviated from the government's line throughout the regulatory process. In the initial phase it took a more liberal approach to entry into Norway, and later it opposed the closure of kindergartens and schools. In late April 2020 Norway began to lift the restrictions, and most institutions and businesses reopened, but a few restrictions remained in place. This changed again in October, with the advent of the second wave and again from February 2021 when the third wave hit, leading to strong re-regulatory measures, before deregulation began again from May.

As of the end of September 2021, a total of 189,000 people out of a population of 5.3 million had been infected (NIPH 2021a) and a total of 861 people had died, which is fewer than in a normal flu season. Norway had one of the lowest scores in Europe with respect to most indicators of the spread of the pandemic; in the Nordic countries only Iceland scored lower, with Finland on a par, Denmark slightly higher and Sweden much higher (Pierre 2020). The overall good performance of Norway and of most of the Nordic countries has been attributed to a number of contextual factors: the Nordic region is sparsely populated and economically affluent, it has good health care systems, and its populations consist by and large of well-educated, disciplined citizens who follow government advice and regulations (Christensen and Laegreid 2020a).

So far, only the preparation and the first regulatory phase in the first wave, has been evaluated by an official corona commission (see Kvinnsland et al. 2021). Its preliminary conclusions were rather damning. First, the commission concluded that the country had generally been poorly prepared. The government had had neither comprehensive contingency plans for a pandemic nor people with the requisite training, not to mention the lack of medical equipment, even though the commission pointed out that COVID-19 had been around for a few months before it was declared a pandemic. The commission also concluded that the decisions connected to the first major draconian measures were taken in a process characterized by a lack of preparation, separate initiatives, lack of coordination, and uncertainty, and had been rushed through on a very tight timeframe. Given all this criticism, it is rather paradoxical that the commission concluded that the Norwegian government had handled the pandemic well, without really stating which criteria this conclusion was based on.

The Norwegian government's overall strategy to control the pandemic was called "testing, isolation, contact-tracing and quarantine" (TISK) (NIPH 2021b). A key part of TISK was the use of digital contact tracing, with the app "Smittestopp." As mentioned, the app came in two versions:

Table 1. Overview of number of infections and numbers related to Smittestopp throughout the COVID-19 pandemic in Norway.

Month	Registered infections every month	Cumulative No. of registered infections	Cumulative No. of downloads of Smittestopp 1 & 2	Cumulative No. of registered infections in Smittestopp 1 & 2
February 21, 2020	1	1	N/A	N/A
March 2020	5,105	5,106	N/A	N/A
April 2020	2,679	7,785	716,000 (April 16)	0
May 2020	633	8,418	1,288,439	0
June 2020	465	8,883	1,577,552 (June 16)	0
July 2020	425	9,308	N/A	0
August 2020	1,617	10,962	N/A	0
September 2020	3,219	14,181	N/A	0
October 2020	7,000	21,181	N/A	0
November 2020	15,481	36,662	N/A	0
December 2020	13,554	50,216	117,700 (Dec. 22)	23
January 2021	13,176	63,392	259,000	203
February 2021	8,723	72,115	692,100	741
March 2021	24,869	96,984	878,900	1,230
April 2021	16,631	113,615	983,800	2,402
May 2021	12,091	125,706	1,006,100	3,047
June 2021	6,265	131,671	1,022,500	3,584
July 2021	6,446	138,117	1,037,400	3,841
August 2021	23,749	161,866	1,047,200	4,054
September 2021	27,969	189,835	1,075,700	4,725
October 2021	18,298	208,133	1,084,500	5,306
November 2021	63,319	271,452	1,087,500	5,650
December 2021	126,236	397,688	1,096,800	7,658
January 2022	408,571	806,259	1,116,300	11,620
February 2022	458,707	1,264,966	1,295,000	29,486
March 2022	142,127	1,407,093	1,308,700	41,946

Source: Data from the Norwegian Institute of Public Health (see NIPH 2021a; 2021c).

the first, Smittestopp 1, was announced in March 2020, launched in April 2020, and eventually banned in June 2020 by the DPA. At this point approximately 1.57 million (out of 5.4 million) Norwegians had downloaded the app, with 600,000 active users (NRK 2020a). Smittestopp 2 was announced in October 2020 and launched in late December 2020. By September 2021, 1.07 million Norwegians had downloaded the app, with fewer than 100,000 downloads in the last six months. During the winter of 2021–2022, the numbers rose slightly (Table 1).

Methods

Because the two versions of the app were created using very different processes, we applied a comparative logic in this case study. We compared the two processes and their outcomes and related these to legitimacy. To do this, we used mainly qualitative data based on documents and interviews. Documents revealed the communication among the various actors involved in developing the two versions of the app. Government statements, official reports (such as the official report by the government-appointed expert evaluation commission (Kvinnsland et al. 2021)), project documents and media reports all provided general information about the management of the coronavirus and the apps. The Norwegian context is characterized by high transparency in public sector decision-making, so it was easy to gain insight into these decisions. In addition, we conducted fifteen interviews with major actors in NIPH, Simula and the DPA who were involved in developing the apps. We also relied upon the interviews conducted by the commission with thirty-five top administrative and political leaders involved in the crisis management of the pandemic in Norway. The interviews provided insight into key decisions made during the crisis and regarding the technology, and outlined the various perspectives on how to use digital technology to combat virus infection. Some quantitative data were used to display the infection numbers in

Norway, the number of downloads and the number of app users, as well as how many cases of infection had been reported through the app.

Legitimacy can be difficult to operationalize, and scholars often use specific empirical measures that only apply in a given context (Weatherford 1992). For a government policy to be legitimate, one would usually think that it must solve a societal problem (Wallner 2008). In our case, the effectiveness of a voluntary contact-tracing app depended first and foremost on citizens downloading it. Downloading an app is a deliberate and conscious act by a citizen who thinks that this is a necessary measure to combat the corona crisis by tracking infections more efficiently. Given that they know of the app, downloading it is an action that legitimizes the measure. If citizens refrain from downloading the app, this indicates that for various reasons they do not think this is a good policy, i.e., not a proper way of dealing with the crisis. Downloading it is thus an operationalization of legitimacy, primarily output legitimacy, because it indicates a willingness to listen to the government's recommendations, which then supposedly translates into more effective crisis management. In a crisis context, it may be the responsibility of the government to convince citizens to download the app, even if this is ultimately voluntary.

Furthermore, the Norwegian health authorities claimed that 60% of the population needed to download the app for it to have an adequate effect and make infection tracking more efficient (NRK 2020b). We can thus compare the number of downloads with this desired number and consider the difference between the two.

Main process features regarding governance capacity and legitimacy

Governance capacity in the contact-tracing apps

Smittestopp 1

At the beginning of the COVID-19 pandemic, the Norwegian government was hesitant about implementing draconic measures (Christensen and Laegreid 2020a). It eventually became clear that it would be possible to create technology which could assist infection detection and provide information that could help the government to assess the effect of the various measures, as well as establishing a knowledge base in preparation for future pandemics (Budd et al. 2020). The early stages of the crisis were a time of great uncertainty and there was no technical experience in Western countries with using mobile phones to track infections (Storeng and de Bengy Puyvallée 2021). The only knowledge to draw on was a research article issued by Oxford University in March 2020 describing the potential of such technology (Ferretti et al. 2020).

Several actors were involved in developing the first version of Smittestopp. Simula, a public research institute in Norway, had offered its IT expertise to the NIPH the day before the draconian measures were implemented in Norway. The NIPH informed Simula about the need for an infection-tracking app and asked it urgently to develop such an app for Norway. In Norway, such requests are usually put out to tender, by law, but NIPH believed that this development had to be done quickly. Also, it became clear that privacy was an important issue in this method of dealing with the crisis, so the Data Protection Authority (DPA) was contacted. On March 27, a regulation tailored to this app was issued by the Ministry of Health (MH), which established the purposes of the app and imposed limits on which data could be collected, how long the data could be stored and what it could be used for.

Smittestopp 1 was launched on April 16. Technologically, it involved GPS tracking, Bluetooth and central data storage. This was done with the aim of both digitally track infection to partly reduce manual infection tracking, and to collect data to assess the effect of the other measures (Kvinnsland et al. 2021:196; Simula 2020). The code was not open source, meaning no outsiders could check the quality of the app. This runs counter to general IT practice and it prompted criticism from the Norwegian public and outside experts (NRK 2020c). About one month after

launch, an independent expert group who got access to the code found that the app did not take sufficient account of privacy considerations. Furthermore, the DPA continually emphasized the importance of transparency, so-called "privacy-by-design," i.e., securing privacy within the technology from the start, as well as general privacy assessments. In retrospect, the head of the DPA said in an interview that "*We got the opportunity to provide input, but it was probably not the case that those inputs were listened to.*"

On June 12, the DPA notified the NIPH that it would ban the app because it did not comply with the General Data Protection Regulation (GDPR). They said that GPS tracking and central storage of data had unclear benefits for Norwegian society and that privacy protection were inadequate. Formally, it was banned in July 2020 and NIPH deleted all the data it had collected.

Smittestopp 2

After the ban, the NIPH was still keen to use infection-tracking technology and therefore sought other ways to do this. As both the development process and the technology itself had been criticized by the public and experts in Norway, it decided to take an alternative approach. NIPH lowered its ambitions and would now only digitally track infection to supplement the Norwegian municipalities' manual tracing and tracking efforts, and not collect data to assess the effects of the other measures (Kvinnsland et al. 2021:201).

In September 2020, NIPH restarted work on the app by putting it out to tender. In October, it was decided that the private firm Netcompany would be responsible for the technical development of the app (NIPH 2020). The process of creating version 2 of the app was very different, a head of department in NIPH explained in an interview. First, more actors were consulted or directly involved throughout. Various professional councils provided input for the app, for instance the Norwegian Computer Society, who were among the experts most critical of the first version. In addition, user groups such as the Norwegian Association of the Blind were also included (NIPH 2020). In interviews, actors in the DPA said that they were updated on assessments made by the NIPH throughout and stated that the DPA was satisfied with the documentation it had received regarding risk and impact assessments.

Second, the technology itself was completely different from the first version, and was now based on an Apple/Google framework (Sharon 2021). This meant that only Bluetooth (rather than GPS) was used to track infections, and the data was stored decentralized on citizens' phones (Ahmed et al. 2020; Grekousis and Liu 2021). This was in line with similar apps in other European countries (EC 2021). Additionally, open source was used, meaning anyone could check the functionality of the app. Hence, there was a high degree of transparency both in the development process and in the technology itself. As the DPA stated that it was satisfied with the data privacy provision in the app, it was launched on December 21, 2020.

The Norwegian health authorities were confident that the technology would contribute well to infection tracking and that many would download the app, as infections had increased a lot during the autumn compared with very low infection numbers during the summer. However, five months after the launch, in June 2021, only 19.2% of Norwegians had downloaded the app (NIPH 2021c).

Looking at the two apps, governance capacity improved in Smittestopp 2 compared with Smittestopp 1. The overall crisis context was a little different, since there was more uncertainty in the first phase, while in the second phase the government knew more about COVID-19, but infection numbers were also higher. As already mentioned, the first app was widely criticized by experts, making legitimacy-building extensive for the second version.

Although the time perspective was relatively short, about half a year between the two "start phases" of the apps (March vs. October 2020), a significant amount of learning related to governance capacity seems to have taken place. The Norwegian government was better prepared for the

Table 2. Comparing governance capacity in the two versions of Smittestopp during the COVID-19 pandemic.

Contextual overview	Smittestopp version 1	Smittestopp version 2
Time period	March–June 2020	October–December 2020, and to date
Uncertainty / infection rate	High uncertainty—medium infection rate.	Medium uncertainty—high infection rate.
Technology	GPS tracking, Bluetooth, central data storage.	Bluetooth and decentralized data storage.
Governance capacity		
Analytical	Low: no knowledge of using technology to track infection (nationally or globally). Uncertainty about effects (GPS vs Bluetooth) and about the crisis in general.	Medium: knowledge gained by experimenting with technology and looking to other countries with similar apps. Also, standards set by MIT Review and Amnesty. Still some uncertainty about effects.
Regulation	High: Involving GPS tracking and central data storage. Heavily surveillance oriented.	Medium: Designed to track infection when citizens register with the app. Does not provide data for evaluating other measures. Privacy ensured.
Coordination	Low: poor vertical coordination by NIPH/ Simula with parent ministry. Lack of inclusion of/ disagreements with DPA (horizontal coordination) and outside experts.	High: NIPH clear on what technology to use; better coordination with ministry and new developer Netcompany. Better inclusion of DPA, outside users and experts.
Service delivery	Low: technology banned after two months by DPA and thus unavailable to citizens.	Low/medium: "approved" by DPA but took long time to be available compared to other measures.

implementation of Smittestopp 2, and governance capacity appears to have been higher in all respects. Table 2 provides an overview of the comparison of the different governance capacity aspects pertaining to the two versions of the app.

Analytical capacity, meaning the government's use of expertise and knowledge (Lodge and Wegrich 2014), was developed throughout the crisis and contributed to reducing uncertainty regarding the technology. This must be understood in the context of other measures, and not just in relation to technology. Over time, the combined effects of social distancing, handwashing, quarantine and border controls had reduced the spread of infection in Norway (Christensen and Laegreid 2020a:775–777). Norway was also able to learn from other countries, both from those with more positive experiences such as China and Singapore, and those with negative experiences such as Spain and Italy (Shi et al. 2022; Tian et al. 2020). Some knowledge of the technology was country-specific, and the health authorities gradually understood what kind of surveillance mechanisms the Norwegian population would accept. While the first app was in operation, there were major debates in the media, with IT-experts contributing different perspectives on surveillance technology. They were very skeptical about the amount of monitoring the Norwegian government wanted to do (Sandvik 2020a:7). In retrospect, Simula in particular blamed these "activists," together with Amnesty International, for spreading lies about the app and disrupting crisis management (Sandvik 2020b; Digi 2020).

Furthermore, digital tracing technologies were also implemented in other countries, which provided some knowledge on their effects and on the public acceptance thereof. The effects of the Bluetooth technology were not entirely clear, even after the implementation of Smittestopp 2 (Grekousis and Liu 2021:9; Xia and Lee 2020). Nevertheless, uncertainty was not completely eliminated because, as Table 1 shows, infections in Norway increased quite a lot around the time when Smittestopp 2 was developed. Overall, analytical capacity increased somewhat from the first to the second version of the app.

Concerning *regulatory capacity*, government surveillance of citizens changed considerably between Smittestopp 1 and Smittestopp 2. In the first version, the health authorities looked at the potential that technology could provide in terms of tracking infections if the entire population were monitored. This entailed very high capacity because the app provided an almost complete overview of every citizen's movements (Grekousis and Liu 2021). In the second version, after the Norwegian DPA deemed the first version illegal, the health authorities chose to limit this capacity, by replacing GPS with only Bluetooth technology, and centralized with decentralized data storage (NIPH 2021d). Capacity was thus limited in the second app, which can be understood in relation to legitimacy, as we discuss below.

In Smittestopp 1, *coordination* capacity was not high. While Simula and the NIPH appeared to be on the same wavelength in developing the technology, there was a lack of horizontal coordination with the DPA. The latter's low involvement meant it was unable to convince the developers about the privacy values and standards required for the app to be accepted. Furthermore, the lack of vertical coordination became evident when the MH issued a legislation for the technology that ended up being inconsistent with existing laws.

Coordination capacity was much higher in Smittestopp 2. Several key actors were now involved after the app was put out to tender, in order to ensure that the technological components would fulfill the efficiency, data security and privacy requirements. The involvement of outside experts, the DPA, and affected groups also ensured legitimacy.

With regard to *delivery capacity*, Smittestopp 1 was banned and unavailable to citizens before it could properly be used, while measures like social distancing, handwashing, quarantine, and border controls were available and in use. For this reason, capacity was slightly higher in Smittestopp 2. This version was at least available over a longer time period to the public, even though it took much longer time for the app to be available. Nevertheless, far fewer people downloaded it (see Table 1), despite the fact that its launch coincided with a rapid increase in infection in Norway, and with the strategic work of the health authorities to get people to download the app. A director in NIPH who oversaw the development of Smittestopp argued this was because "*you have the infection numbers themselves, they are a deterrent,*" and "*in Norway, we are very very good at manual infection tracking … so if you still see that you are contacted very quickly by an infection tracking team, then it is not obvious that you think you should also use the digital tool.*"

Governance legitimacy in the contact-tracing apps

Smittestopp 1

Norway is described as a high-trust society, where citizens generally trust the government. At the beginning of the crisis, major decisions were made under conditions of great uncertainty (Christensen and Laegreid 2020a). This also applied to the technology. While the general decisions were made by the political leadership in collaboration with the NIPH and the Norwegian Directorate of Health (NDH) and were over all accepted by Norwegian citizens, the decision to initiate Smittestopp 1 was made primarily by the NIPH. Director General of the NIPH Camilla Stoltenberg said in an interview with the commission that "*we played a major role in the sense that we were the driving force and initiator to create this infection app.*" Decision-making processes in the Norwegian government are usually open and transparent, but the process of developing the first version of the app was closed with few internal participants, which could potentially undermine legitimacy. In addition, during the development phase when it became evident which technology would be used, the app was rated among the worst contact-tracing apps in the world by Amnesty International and MIT Technology Review (Amnesty 2020; MIT 2020).

Nevertheless, NIPH and Simula continued to emphasize the value such technology could have for infection tracking if many people used it. They said that up to 60% of the population would

have to use it for it to have an adequate effect and efficiently assist infection tracking (NRK 2020b). Both stated publicly that it was vital to use GPS to be able to trace the transmission of the virus quickly. When asked by the media why they did not copy Singapore's app, which was based on open source and Bluetooth, the NIPH said that Smittestopp had been developed for Norwegian conditions and was based on trust between citizens and the government in Norway (NRK 2020c).

In addition, the Norwegian prime minister said at a press conference in April 2020 that "if we want to get our everyday life and freedom back, as many people as possible must download the app" (VG 2020). These measures can be interpreted as an attempt to re-legitimize a process with otherwise low legitimacy. When the technology was banned, the outcome naturally followed in the same way, with low legitimacy. After the app was banned, the Director General of the NIPH said she believed it would weaken crisis preparedness, and the Minister of Health said that he disagreed with the DPA and blamed it for the failure of Smittestopp 1 (Dagbladet 2020). This may have potentially confused citizens and weakened their support.

Smittestopp 2

Legitimacy was strengthened during the development phase for Smittestopp 2. This is evident from the openness surrounding the process, the inclusion of affected groups and privacy experts, and the approval by the DPA. In the tendering process, only one firm wanted to take on the responsibility of creating the new app. Other IT companies in Norway explained that it would pose too great a risk to their reputation to be involved in this process, which was not reassuring. After it had become clear that Netcompany would be the technology developer, it said the communication work it would now have to do was just as important as creating the app itself, and that trust must be built between the Norwegian population and the app (NRK 2020d). This shows once more the importance of public acceptance of such an app.

In Smittestopp 2, the Norwegian health authorities worked more strategically than with Smittestopp 1 to get the population to download the app, a director in the NIPH said in an interview. The leaders recognized that the communication about the previous app had not been very strategic, and that it instead had been simply one item in a long list of advice on infection control, given at daily press conferences. This time, the government hired the advertising agency Dinamo, which promised to conduct a "ruthless" campaign to get as many citizens as possible to download the app (Kampanje 2020). Together, the NIPH, the NDH and Dinamo ran many TV commercials and social media campaigns to image-build and play on people's desire to be able to meet with their families, attend events and send their children back to school. The campaign claimed that the app would help to "bring everyday life back" (Kampanje 2020). The message was conveyed in videos by everyday Norwegians, foreigners speaking other languages and celebrities enthusing about the app. In total, it was communicated in forty-three languages. The idea was to emphasize the necessity of the technology, to spread awareness of it, reach a broad audience, and gain public acceptance.

Furthermore, while there was less uncertainty about the crisis when Smittestopp 2 was developed, the infection numbers were also higher during this period. Nevertheless, Smittestopp 2 was not used very much and contributed little to infection tracking. Couched in terms of legitimacy, the output legitimacy of Smittestopp 2 remained low despite the development phase having higher legitimacy, and the health authorities making a more strategic effort to build legitimacy.

Table 3 summarizes the legitimacy in Smittestopp 1 and 2. The findings regarding governance legitimacy between the two versions of the contact-tracing app are interesting. While public support for the Norwegian government and its overall crisis management was high during the crisis (Christensen and Laegreid 2020b), this was not really reflected in the technology. In the second version of the app, input and throughput legitimacy were higher than in the first, but output legitimacy remained low.

Table 3. Governance legitimacy in the Smittestopp apps.

Governance legitimacy	Smittestopp version 1	Smittestopp version 2
Input	Low: no involvement of outside experts or users in the technological development.	Medium: involvement of the experts who had criticized the first version as well as vulnerable groups.
Throughput	Low: Closed process, no open-source code, no tender process, little involvement of DPA. Expert group found privacy issues.	High: Open-source code, put out to tender, DPA "approved." Strategic work to build legitimacy through TV and social media campaigns.
Output	Low: Did not meet technological expectations of DPA or outside experts. Eventually banned.	Low: Technology was accepted, but still little use made of the app. Not much open public support.

As with governance capacity, there was notable learning involved related to legitimacy between Smittestopp 1 and Smittestopp 2. In the first version, new technology was tried out and the government assumed that the public would support the app because it was a part of other measures requiring a collective effort (Christensen and Laegreid 2020a:777). After the app was banned, the health authorities learned that they had to be more strategic in trying to build, or rebuild, the legitimacy of the app.

Regarding *input legitimacy*, there were few key actors involved in the process of creating Smittestopp 1. No affected groups or IT experts participated. In Smittestopp 2, many of the IT experts who had been especially critical of the first version were consulted, and the inclusion of affected groups gave digitally vulnerable citizens a sense of participation in government action.

There were major changes in *throughput legitimacy* from Smittestopp 1 to Smittestopp 2. First, the source code was changed from being closed to open. The developers of the first version, Simula, had argued in favor of a closed code for data security reasons, but the NIPH changed this in the second version, as seen in Table 2. Furthermore, the design of the app was not put out to tender in the first version, but it was in the second. One of the main criticisms of the first version of Smittestopp by the DPA was that the NIPH had not documented the usefulness of the app or justified the necessity for GPS. In the process of developing the second version these aspects were resolved satisfactorily, according to the DPA (DPA 2021). Additionally, the NIPH worked much more strategically to get citizens to download the second version of the app. Overall, the throughput legitimacy can be regarded as much higher for the second version than for the first.

Output legitimacy was low in both versions and did not improve. Although input and throughput legitimacy together with governance capacity generally improved, output legitimacy, somewhat surprisingly did not change. Downloads of Smittestopp 2 did not reach 75% of those of Smittestopp 1 (see Table 1), even after more than nine months, meaning that citizens were not very willing to follow the government's recommendations with respect to this policy.

Discussion and conclusion

The main findings of our study are that even though there were improvements over time in the processes of governance capacity and legitimacy for the digital contact-tracing technology in Norway, the app did not have a significant role to play in the management of the pandemic, and it did not live up to the expectations of the Norwegian health authorities. If used correctly, such technology can decrease the spread of infection significantly, reduce the strain on health services and assist in crisis management (Abueg et al. 2021; Kucharski et al. 2020).

While infection rates, the level of uncertainty, and government strategies all changed throughout the COVID-19 pandemic, using digital technology to combat the crisis was just one of many possible measures (Hale et al. 2020). It represented a completely new way of dealing with the spread of infection, making the intra-crisis learning curve significant in terms of knowledge gained, technical

functionality, and effects. For such a new approach legitimacy is likely to be paramount when it affects fundamental values regarding the relationship between the government and its citizens.

The main challenge for the government was to get citizens to download and use the app, regardless of which version. Unsurprisingly, there seems to be a connection between the capacity of the app and the level of intrusiveness, making the appropriate balance between privacy and surveillance difficult to achieve for governments, and the strategic work complex (Grekousis and Liu 2021). Looking back at Tables 1 and 2, we can see that there was a long interval between the ban of the first app and the launch of the second, meaning that there was time to assess existing knowledge, look at the experiences of other countries and evaluate alternatives over a relatively long period. The health authorities ended up aiming for moderate capacity with a higher degree of privacy in an attempt to gain legitimacy.

Looking at our empirical case, hiring a different company to develop the technology for the second version of the app for the NIPH was indicative of greater coordination, and it had effects. While Simula had continually argued in favor of its surveillance choices and claimed everything was in order, Netcompany realized that legitimacy had been lost in the first process and that it had to work proactively to restore it in the second. It drew on its experience from a similar app it had developed in Denmark where privacy considerations appeared to be vital for such an app to be accepted by citizens. Together with the health authorities' experience from the Norwegian case, this led to changes in governance capacity in Smittestopp 2, demonstrating the importance of carefully selecting who is involved in coordination, in order not only to coordinate in the right way, but also with the right actors. Overall, this shows the impact of coordination, analytical, regulation and service delivery capacity on legitimacy (Christensen et al. 2016).

Furthermore, the significant changes and improvements in capacity and input and throughput legitimacy between Smittestopp 1 and 2 would, in the best of all worlds, suggest an increase in output legitimacy in the second version. Contrary to expectations, however, this did not occur, and the downloads of the app reached only 20%, which is far from the 60% goal that the NIPH had (NRK 2020b).

As the premise of this type of technology is based on voluntariness, it is only effective when the government and citizens work together. Because of this, both governance capacity and governance legitimacy are central to the development of technology, and important prerequisites for citizens to be able to accept and use such a measure.

Viewing the two apps in relation to the other government measures within the overall TISK strategy of the Norwegian government, some interesting points are relevant to discuss. First, there are some important contextual differences between the two different time-periods when developing the apps. In the period when developing Smittestopp 2, the measures were generally less intrusive, until the end of October 2020 (NOGOV 2020). Although there was a second wave of infection from November 2020, there were many businesses still open, albeit with reduced opening hours, and requirements of distancing and the use of face masks (NOGOV 2020). Since Norway had performed relatively well so far, and vaccines began to come within reach, the country was perhaps not desperate enough for an additional tool like the app to deal with the pandemic, as the other measures had already proved their worth.

Second, one of the ideas of the first Smittestopp app was that it was also supposed to contribute with data, so that the NIPH could research and evaluate the effects of all aspects of the TISK strategy. The Norwegian government had thus aimed toward very high capacity for crisis management at the cost of some privacy, as mentioned earlier. In Smittestopp 2 the ambitions were lowered, as this was not a feature that was possible due to privacy issues, and some of the purpose from the original app vanished. As the second app was more focused on just tracing infection, it was not supposed to replace manual infection tracing, which was one of the goals in the first app, but it was supposed to supplement manual infection tracing (Kvinnsland et al. 2021:196; Simula 2020).

Overall, it does not seem like the Smittestopp apps had a huge impact on the overall TISK strategy of the Norwegian government. This is something that the official corona commission also notes (Kvinnsland et al. 2021). The fact that the commission wrote very little about the app, only about one page in total in a report of 456 pages, can be interpreted as meaning the app did not play a major role in dealing with the pandemic. The commission said that the first app never relieved the municipalities' tracing and tracking efforts, as it was intended to do (Kvinnsland et al. 2021:201). The commission did say that since there was no similar technology available, such an app was a positive initiative. However, they were critical of the fact that privacy considerations were not carried out from the start (Kvinnsland et al. 2021:201).

Nevertheless, one must be careful in declaring success or failure for such a measure in isolation. The overall measures of the Norwegian government's TISK strategy, including distancing and the use of face masks, also partly based on citizens' willingness to follow rules, seems to have worked well, according to the commission (Kvinnsland et al. 2021). While it was experimental from the outset, some lessons were learned throughout the pandemic, which may improve future crisis management. If or when a new pandemic or crisis occurs, one should on the one hand expect that governance capacity with regard to digital technology from the start of a new crisis is higher, something which may also lead to higher legitimacy and acceptance from citizens. It is conceivable that the intra-crisis learning that occurred in this situation may eventually become post-crisis learning, which can then be useful for future crisis management.

On the other hand, it may also be that since this measure did not achieve its intended goal, citizens are now more concerned about government intervention directly into their daily lives and more aware of their privacy in general. With privacy also gaining more public attention with the introduction of the EU's GDPR in 2018, in addition to the fact that citizens may be tired of the pandemic and the other government measures, this can then lead to more difficulties with the acceptance of similar measures or technologies in the future. What emerges from our study is that there may be many factors that affect whether citizens accept a measure or not, and the dynamics within a specific measure and between measures are important to understand for crisis management.

At a general level, one can imagine that capacity and legitimacy sometimes reinforce each other (Christensen and Ma 2021). We see this in our study—with increases in both capacity and some aspects of legitimacy—but there is also evidence in our analysis of legitimacy considerations getting in the way of capacity, creating an opposite effect where the need for legitimacy inhibits capacity. This is illustrated by the reduction of regulatory capacity from Smittestopp 1 to Smittestopp 2. Even though the app was approved in the second process, it had lower capacity in terms of infection tracing. The somewhat low output legitimacy, seen in the actual number of downloads compared to the desired goal of NIPH, appears to persist from the first process to the second, becoming an aspect the Norwegian health authorities had to take into account when trying to convince citizens to download the app (Christensen and Laegreid 2020b).

It is easy to think that output is the most important aspect of crisis management, but our evidence suggests that one should not underestimate input and throughput legitimacy as significant preconditions for output legitimacy. This may apply not only to the use of technology, but also to the general management of crises, where learning and adaptation throughout a crisis occur (Antonacopoulou and Sheaffer 2014; Ansell and Boin 2019).

Additionally, this may also be another argument for allocating more time and resources to the initial crisis response, in order to build analytical capacity early to increase success chance, and thus to mitigate the potentially negative consequences of failing a policy early and not getting it in place until much later in the crisis. Through experience and knowledge building the government can gain a more informed understanding of which measures can successfully be changed or reworked within a crisis (Antonacopoulou and Sheaffer 2014:10), and which measures may be more problematic to change. Along with the coordination of relevant actors and inclusion of citizens in the policymaking process at an early stage, this may more easily ensure the legitimacy of government

measures, at least in terms of digital contact-tracing and possibly other potentially intrusive measures. Overall, this way of viewing legitimacy provides insights into the complex interaction between different types of governance capacity and different types of governance legitimacy (Lodge and Wegrich 2014), and suggests that under certain conditions, considerable improvement in governance capacity can still generate an unsatisfactory output that citizens do not embrace.

As Norway, with high trust in government and low population density, was seen as a high performer in the pandemic. one can question the necessity of a contact-tracing app. It is not obvious that the government should jeopardize the legitimacy of the overall crisis strategy by being more intrusive in citizens personal lives. Nevertheless, it is not known what the pandemics and crisis of the future will bring, and even if the technology itself did not reach the ambitions of the government, the lessons learned from its development process and the citizens' response can be useful.

There are some limitations of this study and opportunities for future research. Our study concerned governance capacity and legitimacy of one measure in a crisis, which has value because it is a study of a novel technology, but it would also be useful to in-depth compare this with capacity and legitimacy of other measures to gain a more holistic appreciation. Another challenge is the operationalization of output legitimacy as downloads of the app. It does not account for people who no longer use the app, meaning that the low legitimacy we have elaborated on here may be even more significant.

Viewing our study in a larger perspective, it would be interesting to do comparisons across countries and not just within a country. This would provide further insight into how governance capacity relates to legitimacy when it comes to technology development by different governments. Understanding the conditions under which such technology thrives or fails is important for future crisis management. While an app similar to Smittestopp but more intrusive was widely used in China, Singapore's app was initially more privacy focused but gradually became more intrusive (MIT 2020). In Europe, Germany greatly limited data collection from the outset. There are thus potentially many different capacity and legitimacy approaches to digital contact-tracing, and it may be interesting to see this in connection with other contextual factors such as a country's surveillance history (Bennett and Raab 2006) or administrative tradition (Painter and Peters 2010), particularly related to e-government. Finally, future research should study the governance capacity and legitimacy of other digital technologies in other crises to enhance our understanding of the use of technology in crisis and disaster management.

Notes on contributorss

Jonas Lund-Tønnesen is a PhD fellow at the Department of Political Science, University of Oslo, Norway. His research interests include digital governance, public management and crisis management.

Tom Christensen is Professor Emeritus at Department of Political Science, University of Oslo, Norway. He is also Visiting Professor at Renmin University and at Tsinghua University, China. His main research interests related to central civil service and comparative public reform studies. He has published extensively in the major PA journals and co-authored several books. His last publication, with Per Lægreid and Kjell Arne Røvik is "Organization Theory and the Public Sector" (Routledge, 2020).

ORCID

Jonas Lund-Tønnesen http://orcid.org/0000-0002-4544-7266

References

Abueg, Matthew, Robert Hinch, Neo Wu, Luyang Liu, William Probert, Austin Wu, Paul Eastham, Yusef Shafi, Matt Rosencrantz, Michael Dikovsky, et al. 2021. "Modeling the Effect of Exposure Notification and Non-

Pharmaceutical Interventions on COVID-19 Transmission in Washington State." *Npj Digital Medicine* 4(1): 1–10. doi: 10.1038/s41746-021-00422-7.
Ahmed, Nadeem, Regio A. Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke, and Sanjay K. Jha. 2020. "A Survey of Covid-19 Contact Tracing Apps." *IEEE Access* 8:134577–601. doi: 10.1109/ACCESS.2020.3010226.
Alemanno, Alberto. 2020. "The European Response to COVID-19: From Regulatory Emulation to Regulatory Coordination?" *European Journal of Risk Regulation* 11(2):1–316. doi: 10.1017/err.2020.44.
Amnesty. 2020. "Bahrain, Kuwait og Norge har de verste korona-appene." Amnesty International. Retrieved March 28, 2021 (https://amnesty.no/bahrain-kuwait-og-norge-har-de-verste-korona-appene).
Ansell, Chris, and Arjen Boin. 2019. "Taming Deep Uncertainty: The Potential of Pragmatist Principles for Understanding and Improving Strategic Crisis Management." *Administration & Society* 51(7):1079–112. doi: 10.1177/0095399717747655.
Ansell, Chris, Arjen Boin, and Ann Keller. 2010. "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System." *Journal of Contingencies and Crisis Management* 18(4):195–207. doi: 10.1111/j.1468-5973.2010.00620.x.
Antonacopoulou, Elena P., and Zachary Sheaffer. 2014. "Learning in Crisis: Rethinking the Relationship between Organizational Learning and Crisis Management." *Journal of Management Inquiry* 23(1):5–21. doi: 10.1177/1056492612472730.
Askim, Jostein, and Tomas Bergström. 2022. "Between Lockdown and Calm down. Comparing the COVID-19 Responses of Norway and Sweden." *Local Government Studies* 48(2):291–21. doi: 10.1080/03003930.2021.1964477.
Bennett, Colin J, and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd ed. Cambridge, MA: MIT Press.
Boin, Arjen, Paul t Hart, Eric Stern, and Bengt Sundelius. 2005. *The Politics of Crisis Management—Public Leadership Under Pressure*. Cambridge: Cambridge University Press.
Budd, Jobie, Benjamin S. Miller, Erin M. Manning, Vasileios Lampos, Mengdie Zhuang, Michael Edelstein, Geraint Rees, Vincent C. Emery, Molly M. Stevens, Neil Keegan, et al. 2020. "Digital Technologies in the Public-Health Response to COVID-19." *Nature Medicine* 26(8):1183–92. doi: 10.1038/s41591-020-1011-4.
Cerutti, Furio, and Sonia Lucarelli. 2008. "Why Political Identity and Legitimacy Matter in the European Union." Pp. 17–36 in *The Search for a European Identity*. London and New York: Routledge.
Cheng, Hao-Yuan, Shu-Wan Jian, Ding-Ping Liu, Ta-Chou Ng, Wan-Ting Huang, and Hsien-Ho Lin. 2020. "Contact Tracing Assessment of COVID-19 Transmission Dynamics in Taiwan and Risk at Different Exposure Periods before and after Symptom Onset." *JAMA Internal Medicine* 180(9):1156–63. doi: 10.1001/jamainternmed.2020.2020.
Christensen, Tom, and Per Laegreid. 2020a. "Balancing Governance Capacity and Legitimacy: How the Norwegian Government Handled the COVID-19 Crisis as a High Performer." *Public Administration Review* 80(5):774–9. doi: 10.1111/puar.13241.
Christensen, Tom, and Per Laegreid. 2020b. "The Coronavirus Crisis—Crisis Communication, Meaning-Making, and Reputation Management." *International Public Management Journal* 23(5):713–29. doi: 10.1080/10967494.2020.1812455.
Christensen, Tom, Per Laegreid, and Lise H. Rykkja. 2016. "Organizing for Crisis Management: Building Governance Capacity and Legitimacy." *Public Administration Review* 76(6):887–97. doi: 10.1111/puar.12558.
Christensen, Tom, and Liang Ma. 2021. "Comparing SARS and COVID-19: Challenges of Governance Capacity and Legitimacy." *Public Organization Review* 21(4):629–17. doi: 10.1007/s11115-021-00510-y.
Cyert, Richard M., and James G. March. 1963. "A Behavioral Theory of the Firm." *Prentice-Hall International Series in Management*, edited by James G. March, Englewood Cliffs, NJ: Prentice-Hall.
Dagbladet. 2020. "FHI-fiasko: Tvilte i mai." *Dagbladet*. Retrieved May 1, 2021 (https://www.dagbladet.no/nyheter/fhi-fiasko-tvilte-i-mai/72895330).
Digi. 2020. "Simula langer ut." *Digi*. Retrieved May 28, 2021 (https://www.digi.no/artikler/simula-langer-ut-rapporten-de-har-levert-er-direkte-soppel-og-er-et-stykke-elendig-arbeid/500102?key=11YGFJW5).
DPA. 2021. "Årsrapport for 2020." Data Protection Authority. Retrieved June 10, 2021 (https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsrapport-for-2020/).
Easton, David. 1965. *A System Analysis of Political Life*. New York: Wiley.
EC. 2021. "Mobile Contact Tracing in EU Member States." European Commission. Retrieved June 11, 2021 (https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en).
Egeberg, Morten. 2012. "How Bureaucratic Structure Matters: An Organizational Perspective." Pp. 157–68 in *Handbook of Public Administration*, edited by B.G. Peters and J. Pierre. London: Sage.

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing." *Science* 368(6491):6491. doi: 10.1126/science.abb6936.

Gai, Ruoyan, and Makoto Tobe. 2020. "Managing Healthcare Delivery System to Fight the COVID-19 Epidemic: experience in Japan." *Global Health Research and Policy* 5(1):1–4. doi: 10.1186/s41256-020-00149-0.

Grekousis, George, and Ye Liu. 2021. "Digital Contact Tracing, Community Uptake, and Proximity Awareness Technology to Fight COVID-19: A Systematic Review." *Sustainable Cities and Society* 71:102995. doi: 10.1016/j.scs.2021.102995.

Hale, Thomas, Anna Petherick, Toby Phillips, and Samuel Webster. 2020. "Variation in Government Responses to COVID-19." *Blavatnik School of Government Working Paper* 31:2020–11.

Head, Brian W., and John Alford. 2015. "Wicked Problems: Implications for Public Policy and Management." *Administration & Society* 47(6):711–39. doi: 10.1177/0095399713481601.

Kampanje. 2020. "Nytt reklamebyrå får prøve seg i kampen mot korona: - vi kommer til å vaere nådeløse." *Kampanje*. Retrieved May 5, 2021 (https://kampanje.com/reklame/2020/11/nytt-reklamebyra-far-prove-seg-i-kampen-mot-korona--vi-kommer-til-a-vare-nadelose/).

Kostka, Genia, and Sabrina Habich-Sobiegalla. 2020. "In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the United States." *New Media & Society*, https://doi.org/10.1177/14614448221083285.

Kucharski, Adam J., Petra Klepac, Andrew J. K. Conlan, Stephen M. Kissler, Maria L. Tang, Hannah Fry, Julia R. Gog, W., John Edmunds, Jon C. Emery, Graham Medley, et al. 2020. "Effectiveness of Isolation, Testing, Contact Tracing, and Physical Distancing on Reducing Transmission of SARS-CoV-2 in Different Settings: A Mathematical Modelling Study." *The Lancet Infectious Diseases* 20(10):1151–60. doi: 10.1016/S1473-3099(20)30457-6.

Kvinnsland, Stener, Astri Aas-Hansen, GeirSverre Braut, KnutEirik Dybdal, Tone Fløtten, Rune Jakobsen, Toril Johansson, Christine Korme, Nina Langeland, Egil Matsen, et al. 2021. *Myndighetenes Håndtering av Koronapandemien. Rapport fra Koronakommisjonen*. Oslo: Prime Minister's Office. NOU 2021: 6. Retrieved August 13, 2021 (https://www.regjeringen.no/contentassets/5d388acc92064389b2a4e1a449c5865e/no/pdfs/nou202120210006000dddpdfs.pdf).

Lodge, Martin, and Kai Wegrich. 2014. *The Problem-Solving Capacity of the Modern State: Governance Challenges and Administrative Capacities*. Oxford: Oxford University Press.

Marcussen, Marcus. 2010. "Scientization." Pp. 321–33 in *Ashgate Research Companion to New Public Management*, edited by Tom Christensen and Per Laegreid, Aldershot: Ashgate, 99.

Mbunge, Elliot, Boluwaji Akinnuwesi, Stephen G. Fashoto, Andile S. Metfula, and Petros Mashwama. 2021. "A Critical Review of Emerging Technologies for Tackling COVID-19 Pandemic." *Human Behavior and Emerging Technologies* 3(1):25–39. doi: 10.1002/hbe2.237.

Meijer, Albert J., Miriam Lips, and Kaiping Chen. 2019. "Open Governance of Cities: A New Paradigm for Understanding Urban Collaboration." *Frontiers in Sustainable Cities* 1(3):1–9. doi: 10.3389/frsc.2019.00003.

Meijerink, Hinta, Elisabeth H. Madslien, Camilla Mauroy, Mia Karoline Johansen, Sindre Mogster Braaten, Christine Ursin Steen Lunde, Trude Margrete Arnesen, Siri Laura Feruglio, and Karin Maria Nygard. 2021. "The First GAEN-Based COVID-19 Contact Tracing App in Norway Identifies 80% of Close Contacts in Real Life Scenarios." *medRxiv* 3:1–9.

MIT. 2020. «Covid Tracking Tracker." MIT Technology Review. Retrieved March 28, 2021 (https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker/).

NIPH. 2020. "Oppdateringer om arbeidet med nye Smittestopp." Norwegian Institute for Public Health. Retrieved June 2, 2020 (https://www.fhi.no/om/smittestopp/digital_smittesporing/).

NIPH. 2021a. "Statistikk om koronavirus og covid-19." Retrieved April 18, 2022 (https://www.fhi.no/sv/smittsomme-sykdommer/corona/dags–og-ukerapporter/dags–og-ukerapporter-om-koronavirus/).

NIPH. 2021b. "Smittestopp – prosjektbeskrivelse." Norwegian Institute for Public Health. Retrieved October 4, 2021 (https://www.fhi.no/cristin-prosjekter/aktiv/smittestopp/).

NIPH. 2021c. "Nøkkeltall fra Smittestopp." Norwegian Institute for Public Health. Retrieved April 18, 2022 (https://www.fhi.no/om/smittestopp/nokkeltall-fra-smittestopp/).

NIPH. 2021d. "Om Smittestopp." Norwegian Institute for Public Health. Retrieved June 16, 2021 (https://www.fhi.no/om/smittestopp/om-smittestopp/).

NOGOV. 2020. "Timeline: The Governments' Handling of the Corona Situation." Norwegian Government. Retrieved April 18, 2022 (https://www.regjeringen.no/no/tema/Koronasituasjonen/tidslinje-koronaviruset/id2692402/).

NRK. 2020a. "Nesten 1,5 millioner nedlastninger." NRK. Retrieved June 15, 2020 (https://www.nrk.no/nyheter/nesten-1_5-millioner-nedlastinger-1.14997489).

NRK. 2020b. "Bare én av fem deler data fra Smittestopp-appen." NRK. Retrieved April 28, 2021 (https://www.nrk.no/norge/bare-en-av-fem-deler-data-fra-smittestopp-appen-1.15000801).

NRK. 2020c. "Hundrevis av IT-eksperter fra hele verden ut mot sporingsapper som norske Smittestopp." NRK. Retrieved April 25, 2021 (https://www.nrk.no/norge/hundrevis-av-it-eksperter-fra-hele-verden-ut-mot-sporing-sapper-som-norske-smittestopp-1.14988352).
NRK. 2020d. "Det viktigste blir kommunikasjonsjobben." NRK. Retrieved June 2, 2021 (https://nrkbeta.no/2020/10/22/det-viktigste-blir-kommunikasjonsjobben/).
Oliver, Nuria, Bruno Lepri, Harald Sterly, Renaud Lambiotte, Sébastien Deletaille, MarcoDe Nadai, Emmanuel Letouzé, AlbertAli Salah, Richard Benjamins, and Ciro Cattuto. 2020. "Mobile Phone Data for Informing Public Health Actions across the COVID-19 Pandemic Life Cycle."
Painter, Martin, and B. Guy Peters. 2010. *Tradition and Public Administration*. London: Palgrave Macmillan UK.
Pierre, Jon. 2020. "Nudges against Pandemics: Sweden's COVID-19 Containment Strategy in Perspective." *Policy & Society* 39(3):478–93. doi: 10.1080/14494035.2020.1783787.
Rotolo, Daniele, Diana Hicks, and Ben R. Martin. 2015. "What is an Emerging Technology?" *Research Policy* 44(10):1827–43. doi: 10.1016/j.respol.2015.06.006.
Ryan, Mark. 2020. "In Defence of Digital Contact-Tracing: Human Rights, South Korea and Covid-19." *International Journal of Pervasive Computing and Communications* 16(4):383–407. doi: 10.1108/IJPCC-07-2020-0081.
Sandvik, Kristin B. 2020a. "Smittestopp": If You Want Your Freedom Back, Download Now." *Big Data & Society* 7(2):205395172093998. doi: 10.1177/2053951720939985.
Sandvik, Kristin B. 2020b. "Smittestopps vekst og fall: Koronarettssosiologiske observasjoner." Sosiologen.no. Retrieved June 2, 2021 (https://sosiologen.no/essay/korona-stafett/smittestopps-vekst-og-fall-koronarettssosiologiske-observasjoner/).
Scharpf, Fritz W. 1999. *Governing in Europe: Effective and Democratic?* Oxford: Oxford University Press.
Schmidt, Vivien A. 2013. "Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput." *Political Studies* 61(1):2–22. doi: 10.1111/j.1467-9248.2012.00962.x.
Sharon, Tamar 2021. "Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers." *Ethics and Information Technology* 23(S1):45–13. doi: 10.1007/s10676-020-09547-x.
Shi, Lei., Chen Shi, Xun Wu, and Liang Ma. 2022. "Accelerating the Development of Smart City Initiatives Amidst the COVID-19 Pandemic: The Case of Health Code in China." *Journal of Asian Public Policy* 15(2):266–18. doi: 10.1080/17516234.2021.1902078.
Simula. 2020. "Sammenligning av alternative løsninger for digital smittesporing." Simula Research Laboratory. Retrieved April 18, 2022 (https://www.simula.no/sites/default/files/sammenligning_alternative_digital_smittesporing.pdf).
Storeng, Katerini Tagmatarchi, and Antoine de Bengy Puyvallée. 2021. "The Smartphone Pandemic: How Big Tech and Public Health Authorities Partner in the Digital Response to Covid-19." *Global Public Health* 16:1482–98. doi: 10.1080/17441692.2021.1882530.
Taeihagh, Araz, M. Ramesh, and Michael Howlett. 2021. "Assessing the Regulatory Challenges of Emerging Disruptive Technologies." *Regulation & Governance* 15(4):1009–19. doi:10.1111/rego.12392.
Thiele, Lukas, and Andree Pruin. 2021. "Does Large-Scale Digital Collaboration Contribute to Crisis Management? An Analysis of Projects from the# WirVsVirus Hackathon Implemented in Germany during the COVID-19 Pandemic." *Dms – Der Moderne Staat – Zeitschrift Für Public Policy, Recht Und Management* 14(2-2021):334–50. doi: 10.3224/dms.v14i2.07.
Tian, Huaiyu, Yonghong Liu, Yidan Li, Chieh-Hsi Wu, Bin Chen, Moritz U. G. Kraemer, Bingying Li, Jun Cai, Bo Xu, Qiqi Yang, et al. 2020. "An Investigation of Transmission Control Measures during the First 50 Days of the COVID-19 Epidemic in China." *Science (New York, N.Y.)* 368(6491):638–42. doi: 10.1126/science.abb6105.
VG. 2020. "Solberg: - Hvis vi skal få hverdagen tilbake, må flest mulig laste ned appen." VG. Retrieved June 1, 2021 (https://www.vg.no/nyheter/innenriks/i/P9xGAJ/solberg-hvis-vi-skal-faa-hverdagen-tilbake-maa-flest-mulig-laste-ned-appen).
Waeraas, Arild, and Moshe Maor. 2014. *Organizational Reputation in the Public Sector*. London: Routledge.
Wallner, Jennifer 2008. "Legitimacy and Public Policy: Seeing beyond Effectiveness, Efficiency, and Performance." *Policy Studies Journal* 36(3):421–43. doi: 10.1111/j.1541-0072.2008.00275.x.
Weatherford, M. Stephen 1992. "Measuring Political Legitimacy." *American Political Science Review* 86(1):149–66. doi: 10.2307/1964021.
Weick, Karl E. 1995. *Sensemaking in Organizations (Vol. 3)*. Vol. 3. Thousand Oaks, CA: Sage.
Xia, Ye, and Gwendolyn Lee. 2020. "How to Return to Normalcy: fast and Comprehensive Contact Tracing of COVID-19 through Proximity Sensing Using Mobile Devices." *arXiv Preprint arXiv:2004.12576*: 1–12.
You, Myoungsoon, and Youngkee Ju. 2019. "Salience of Public Leaders' "Meaning Making" in News Coverage of a Health Crisis." *Journal of Contingencies and Crisis Management* 27(4):400–5. doi: 10.1111/1468-5973.12259.

Article 3: Privacy regimes, crisis strategies, and governments' legitimizing of digital surveillance technology: Comparing Germany, Norway, and the United Kingdom

Publication status: sent to *International Journal of Public Administration*.

Privacy regimes, crisis strategies, and governments' legitimizing of digital surveillance technology: Comparing Germany, Norway, and the United Kingdom

Jonas Lund-Tønnesen

Abstract

The future trajectory of government surveillance is unmistakable: it is increasing. Yet, despite an increase in implemented surveillance measures, we lack an understanding of how governments legitimize new surveillance measures and why that might vary across countries. This paper argues that ways of legitimizing digital surveillance technology are shaped by privacy regime legacies and overarching strategies of problem-solving when facing a crisis. With a cross-country comparison, the study finds both similar and different legitimacy strategies by governments in Germany, Norway, and the United Kingdom. The analysis demonstrates the significance of historical privacy practices and governmental problem-solving capacities in shaping technological change and future directions for public administration.

Keywords: Covid-19 pandemic; crisis management; governance legitimacy; legitimization; strategic communication.

Introduction

Looking at the past and looking at the present, the trajectory of government surveillance is unmistakable: it increases (Yates and Whitford, 2022). Observers frequently note that the pace of development accelerates during times of crisis, as crises can function as windows of opportunity for governments to introduce (often controversial) surveillance policies (Boersma and Fonio, 2018). To gain and maintain support for such policies, which commonly take the form of digital surveillance technology, governments are generally required to legitimize, persuade, and make sense of their choices (Suchman, 1995; Schulze, 2015; Pauli et al., 2016). If successful in persuading citizens and other stakeholders, there can be long-lasting consequences beyond the single policy, such as institutionalized acceptance, making future mass surveillance policies easier to implement and less disputed. Such technology could increase the government's efficiency by providing important information about citizens and their behavior that can inform public policy decisions (Lund-Tønnesen and Christensen, 2023a), but could also fulfill predictions of a dystopian society. If unsuccessful, negative perceptions could provide implementation constraints, which on paper could prevent efficient decision-making systems, but also ensure some forms of privacy.

Extant research has concentrated much on *citizens*' attitudes and reactions towards general surveillance, as well as specific surveillance tools and agencies (e.g., Davis and Silver, 2004; Rykkja et al., 2011; Degli Esposti et al., 2021), but less on how *governments* use rhetorical devices to shape citizens' expectations, commitments, perceptions and acceptance of such tools. Moreover, the public administration literature has paid more attention to stable situations than unsettled crisis situations and has not focused much on governance legitimacy in relation to digital surveillance technology in crisis management (Boin and Lodge, 2016; Christensen, Lægreid, and Rykkja, 2016; Boersma and Fonio, 2018). Therefore, this study aims to fill these gaps by exploring how governments in three different countries strategically legitimize the same digital surveillance technology in a crisis. The legitimizing of contact tracing apps, which were developed as key tools for infection tracking in Germany, Norway, and the UK in the first stage of the COVID-19 pandemic is compared. These three countries represent different historical privacy regimes – i.e., governance arrangements, practices, and legacies related to privacy protection. The study begins with an assumption that governmental legitimacy strategies are expected to largely depend on trajectories of privacy regimes of the past (Bygrave, 2004; Bennett and Raab, 2006), and that path dependency can explain the adopted strategies (Steinmo et al., 1992). As the study is concerned with these strategies in a

pandemic, it is also expected that the strategies align with the governments' overall crisis responses (Boin et al., 2005; Kuhlmann et al., 2021). Formally, the following questions are addressed:

- *How did governments in Germany, Norway, and the United Kingdom legitimize their contact tracing applications in the COVID-19 pandemic?*
- *To what extent are these approaches in line with the privacy regimes and overall crisis strategies in the three countries?*
- *How can path dependency explain the adopted legitimacy strategies?*

The analysis concentrates on the starting phase of the COVID-19 pandemic, which is roughly March-June 2020. This is a point in time where cross-country learning is in its infancy and a phase where possible convergence between countries has not yet occurred. It is a suitable phase to study variation between countries' legitimacy strategies, as approaches here are expected to be most constrained and enhanced by existing administrative, cultural, and political features (Christensen et al., 2016).

The article is structured as follows: First, three types of legitimacy strategies are identified and outlined. Thereafter, the institutional contexts with key elements related to path dependency, privacy regimes, and crisis strategies are described. This is followed by a description of the methods and data. Next, the results are presented, focusing on the main differences between the countries. Finally, the findings are discussed, and the study is concluded.

Legitimacy strategies

Strategic legitimacy is a fundamental part of gaining acceptance of government policies and managing crises (Lægreid and Rykkja, 2023; Svenbro and Wester, 2023). In general, legitimacy is about citizens' perception or assumption of whether the actions of government are desirable, proper, or appropriate within a socially constructed system of beliefs, norms, values, and definitions (Suchman, 1995, p. 574). Strategic legitimacy is about how certain agents, such as governmental actors, work to establish meaning and shared understanding of a situation, ways of dealing with it and communicating that to the public (Boin et al., 2005; Lægreid and Rykkja, 2023). This process essentially involves three aspects: how legitimacy is gained, maintained, and/or repaired (Suchman, 1995).

Legitimacy strategies in the literature on public discourses more generally are well researched (Van Leeuwen, 2007). This literature shows that legitimacy can be pursued through

different linguistic paths that emphasize values, emotions, and hypothetical scenarios (Reyes, 2011). Approaches are often based on the "collective memory" and "shared beliefs" of actors in a social context (Beasley, 2011), where meaning is created by the use of the past and the current context to justify courses of action (Hart et al., 2005; Reyes, 2011). In relation to surveillance, some research has studied legitimacy and based it on the ideas of Suchman (e.g., Schulze, 2015; Pauli et al., 2016). This literature has predominantly been concerned with scandals, and specifically Edward Snowden's revealing of the American National Security Agency's (NSA) extensive secret surveillance (Schulze, 2015; Lischka, 2017; Tiainen, 2017; Wahl-Jorgensen et al., 2017; Kuehn, 2018). These contributions largely focus on how legitimacy is *repaired* after a scandal, as well as the role of media in this legitimizing. The literature has not focused on attempts at *gaining* or *building* legitimacy in the first place by governmental actors seeking to introduce surveillance measures, or how experiences with surveillance and privacy in the past might shape governments' legitimacy strategies.

To examine this, I first follow existing research that relies on the differentiation by Suchman (1995) and argue that rhetorical approaches can rest on three dimensions of legitimacy: pragmatic, moral, and cognitive legitimacy. These approaches concern what governments strategically focus on, but not necessarily what they achieve in practice. Table 1 provides an overview of the operationalization of these dimensions. I see them as having two main components in rhetorical communication: 1) justifying governments' own practices, and 2) specifically addressing citizens to support, accept, and utilize the digital surveillance technology. The pragmatic dimension rests on assessments of self-interest and utility calculations of the government's immediate audience: citizens. When the government strategically embraces this form of legitimacy it attempts to influence evaluations of self-interest and utility by citizens. Support for a public policy or technology comes from the expected value and benefit for the evaluators (Suchman, 1995, p. 578). The ultimate success of a new technology depends on its technical superiority compared with other means of problem-solving to improve crisis management capacity, and how that superiority is strategically justified and communicated (Suddaby et al., 2017, p. 21). Moreover, when a policy or technology is controversial – as with much of surveillance technology – it can be expected that the government will highlight that its actions are compliant with existing legislation, thereby upholding perceived instrumental demands (Scott, 2014).

Moral legitimacy concerns normative evaluations and approval related to duty and appropriateness (Scott, 2014). Strategically, it is about emphasizing that choices, activities, and

approaches are "the right thing to do" (Suchman, 1995, p. 579). This can entail that the policy or technology is developed according to established standards and that socially accepted approaches and techniques are embraced. Consulting experts is one way of doing this. Moreover, to get citizens to support and use an introduced technology, rhetoric appealing to altruistic ideals such as societal welfare is highlighted in this dimension (Suchman, 1995).

Further, cognitive legitimacy is achieved when an organization or a technology becomes so well-integrated into a social system that its characteristics are deemed natural and uncontested (Suchman, 1995; Scott, 2014; Suddaby et al., 2017). Strategically, this dimension is about framing which solutions are conceivable and inevitable, and which are not. The rationale is that if alternatives to proposed approaches are unimaginable, challengers are fewer in number and easier to persuade. When introducing a new surveillance technology, governmental actors need to construct and alter fundamental beliefs for it to gain acceptance (Suddaby and Greenwood, 2005). The overarching objective of government is then to get citizens to imagine that "for things to be otherwise is *literally* unthinkable" (Suchman, 1995, p. 583, italics in original). In this study, this involves presenting the idea that not using digital surveillance technology would be unthinkable. While constructing and altering such beliefs is difficult (Scott, 2014), situations of high uncertainty, urgency, and ambiguity such as crises present occasions for this type of legitimacy-building (Lund-Tønnesen, 2022). Which of these three different strategies governments adopt regarding digital surveillance technology in the COVID-19 crisis, is expected to be dependent on the pandemic situation, but also the countries' historical legacy in the realm of surveillance and privacy.

Table 1. Operationalization of the dimensions of legitimacy.

Dimension of legitimacy	**Indicator**
Pragmatic legitimacy	**General**: Self-interest, within the law, technological superiority, practical consequences **Specific**: ***Internal conduct***: Follow privacy laws, improve own crisis management capacity ***External influence***: Citizens' own (or relatives') health most important, technical superiority compared with other crisis measures, easy to use.
Moral legitimacy	**General**: Duty, altruism, standards **Specific**: ***Internal conduct*:** Follow standards for relevant technology, consult with IT-experts ***External influence*:** Help community to stop infection from spreading, what is best for society/the common good.
Cognitive legitimacy	**General**: Framing inevitable and inconceivable approaches

	Specific: ***Internal conduct*:** Modern technology obviously must be utilized by government Old ideas of technology challenged ***External influence*:** The only way to overcome the crisis (return to "normality" and regain "freedom") Technology provides a fundamental function in crisis management Difficult to imagine a world without this technology.

Institutional context and legacies of the past

Applying a comparative case study approach, the selected countries are Germany, Norway, and the United Kingdom. These countries are chosen for comparison because they are Western, developed countries with similar fundamental structural characteristics (democracy, functioning bureaucracy, health system, economic system, level of economic development) (Kuhlmann and Wollmann, 2019), and similar data protection laws, within the framework of the EU General Data Protection Regulation (GDPR). Although the UK and Norway are not members of the EU, they have their own identical versions of the GDPR. The countries also share many characteristics in digital developments and reform in the public-administrative apparatus in recent decades, although levels of digitalization differ somewhat (Hammerschmid et al., 2023). It is also worth noting that Germany is a federal state, and that Norway is less populous compared to the other countries. Moreover, measures to deal with the COVID-19 pandemic were introduced at about the same time in the three countries, around March 2020, and importantly, they all developed a digital surveillance technology, a contact tracing app, to combat the coronavirus in the COVID-19 pandemic in the early stages of the pandemic. These apps were part of the governments' overall public health response and were developed for mobile phones to trace the spread of the coronavirus and notify citizens whether they had been in close proximity with infected citizens (Lund-Tønnesen, 2022). They were seen as controversial because of their unclear effects on infection tracing and potential for mass surveillance. The use of the apps was voluntary, implying that there was a need for persuasion by the government for them to be utilized by the population.

While the three countries share the characteristics mentioned above, they differ significantly in their privacy regimes, meaning the set of governance legacies, arrangements, and practices related to privacy, personal data, and data protection (Bennett and Raab, 2006; Boersma et al., 2014). This study assumes that these differences, which are elaborated on in the following, can help us understand the countries' approaches to legitimizing the digital surveillance technology. The theoretical reasoning follows historical institutionalism, which

claims that responses to new problems are greatly influenced by existing institutional conditions and experiences of problem-solving in the past (Steinmo et al., 1992). This approach argues that once choices and ideas are institutionalized in a policy area, those patterns are likely to persist and will function as basic templates for future decision-making, so-called "path dependency" (Steinmo, 2008). The outcomes of policy efforts trigger feedback mechanisms that can reinforce the current trajectory and strong forces are needed to overcome the inertia in the system, often characterized as "critical junctures" (Krasner, 1988; Pierson, 2000). In this study, it is assumed that governments' legitimacy strategies (emphasizing pragmatic, moral, and/or cognitive aspects) must be understood in view of the institutional path dependencies and country-specific historical conditions related to privacy. We can think of the COVID-19 pandemic as a critical juncture, and if legitimacy approaches persist into this crisis, the institutional conditions and legacies in this field are particularly important.

Privacy regimes in Germany, Norway, and the United Kingdom

In a global context, European privacy regulation is often seen as more extensive and bureaucratic compared to other regions, but there are still presumably substantial variations between countries, as with other EU policies (Versluis, 2007). The German tradition of privacy protection has deep roots in ideas of freedom and personality, which can be traced back to the philosophies of Kant, Hegel, and Humboldt (see Whitman, 2004). This became more extensively established in legal and administrative statutes and praxis right after the Second World War. Observers generally view the privacy regime in Germany as among the strictest in the world (Flaherty, 1989; Bygrave, 2004). This view is due to Germany's exceptional focus on following privacy laws, firm constitutional basis for privacy, and general legalistic administrative culture, as well as systematic integration of privacy concerns in ICT systems, established enforcement mechanisms, and history of privacy information officers in organizations. Moreover, Germans take privacy issues seriously, and privacy has been viewed as a necessary condition for citizens' political participation and a thriving democracy (Flaherty, 1989; Bygrave, 2004).

Norway has historical cultural values related to personal freedom and integrity, albeit not as intellectually rooted as in Germany. The country was an early adopter of comprehensive privacy laws, in 1978, and has long been committed to protecting individual privacy rights (Bennett and Raab, 2006). Norway enjoys high social and political trust, which has made Norwegian citizens positive towards the use of surveillance in the fight against crime and terrorism (Rykkja, Lægreid, and Fimreite, 2011). Moreover, the Norwegian government has a

history of both protecting privacy in policy and intelligence registers, but also a history of (partly illegally) surveilling citizens belonging to the political left, up until 1989 (Rykkja et al., 2011). After the turn of the century, the government has frequently proposed to implement the EU data storage directive, but faced massive protests and postponed the implementation indefinitely.

In the UK, it has historically been up to data controllers and not privacy regulations or Data Protection Authorities (DPAs) to assess and balance the common law duty of confidentiality with public interests, in line with their common law principles (Bellamy et al., 2005). During the Cold War, the UK government extensively surveilled political groups and activists. Moreover, administrative reforms at the end of the 1990s created lasting tensions for the government between improving public policies by use of personal data and protecting privacy (Bellamy et al., 2005). The country expanded the surveillance powers of intelligence agencies in 2016, but also implemented the GDPR in 2018. Generally, it is commonly believed that the DPA in the UK is and has been more favorable towards governments' and businesses' information needs compared with other European countries (Yeung and Bygrave, 2022).

Overall, all three countries have experience with surveillance and privacy protection, but in different ways. Germany reportedly has a stricter privacy regime than the other countries, while the UK is somewhat more flexible. The characteristics are summed up in Table 2. The role of crisis strategies, and how these two aspects are expected to shape legitimacy strategies are explicated in the following.

Table 2. Overview of country-specific conditions and expectations.

	Germany	**Norway**	**United Kingdom**
Institutional history of privacy regime	Strict privacy regime (privacy historically engrained in society and legal-administrative rule-following)	Moderately strict privacy regime (historically committed to protecting privacy, but also perceived leeway to implement surveillance measures when needed)	Comparatively less strict privacy regime (sometimes seen as favorable to businesses and data-driven public organizations)
Overarching crisis strategy in the early stages of the COVID-19 pandemic	Suppression approach with partial lockdown, emphasis on voluntary compliance	Suppression approach with partial lockdown, emphasis on no alternative to draconian regulations, and "dugnad"	Liberal strategy, citizens should make their own risk assessments
Expectations for legitimizing the	Predominantly focus on complying with	Stress cognitive dimension more than	Highlight self-interest more than the other

Digital Surveillance Technology	rules and adhering to IT standards. Strongly shaped by privacy legacy and regime. Also, equivalent rules and moral focus following overall crisis strategy.	the others, and moral values of "dugnad". Mostly influence from overall crisis strategy. Some minor focus on rules and standards based on privacy regime.	countries, due to crisis strategy of making own assessments and because of the less rigorous privacy regime legacy.

Overarching crisis strategies

Governments generally have an overall communication strategy as part of their crisis management. However, the communication, legitimizing, explanation, and values that are embraced for individual crisis measures can vary considerably (Christensen and Lægreid, 2020; Boin and Lodge, 2021a). An example of this is that in Norway during the pandemic, the government only emphasized self-interest regarding the use of face masks, which is rather different from the overall strategy, as described below (see e.g., Christensen and Lægreid, 2022). In this paper, the legitimacy strategies concerning digital surveillance technologies are viewed as a sub-strategy of the governments' overall crisis communication strategy. This means that the legitimacy strategies are obviously expected to be shaped by the overall crisis strategy, but that there are variations of the specific measures based on their substantive functions and relation to other measures. This variable is used as a situational variable in this study, which is not uncommon in crisis research where situations are unique, and we need a nuanced understanding of what is going on.

In the COVID-19 pandemic, Germany had an overall suppression strategy with a partial lockdown to handle the coronavirus. The overarching strategy involved implementing legally mandatory regulations together with communicating and encouraging voluntary compliance, with relative coherence of the measures between regions (Kuhlmann et al., 2021). Although regional powers are strong in Germany, many decisions were coordinated at the central level to ensure national standards. Expert institutions and advice played a central role in Germany, and both politicians and experts were active in communicating, explaining, and legitimizing crisis measures (Kuhlmann et al., 2022).

The Norwegian government's overall crisis strategy to deal with the coronavirus was similar to Germany's strategy, with a suppression approach and partial lockdown. The government's communication strategy was generally about appealing to collective action, solidarity, and voluntary work using the slogan "working together" and the Norwegian cultural concept of "dugnad" (Christensen and Lægreid, 2020; Arora et al., 2022). Implementation of

the strict regulations was justified with the argument that there was no alternative to draconian rules and that it was an extreme situation where unusual measures were necessary (Christensen and Lægreid, 2020, p. 719).

The UK initially had a liberal strategy for dealing with the pandemic, where a hard lockdown was not seen as an option (Boin and Lodge, 2021a). Early on, communication from the government was about risk and enabling citizens to make their own risk decisions, and expert advice was not frequently used (Boin et al., 2023, p. 331 and 336). This pandemic response, with its reluctant decision-making compared to other European countries, was frequently criticized by the public and experts and viewed as a governance failure. It highlighted the shortcomings and failures of leadership and communication to the public. Eventually, the lockdown strategy changed, and extensive and intrusive measures were implemented (Boin et al., 2023).

Expectations

Based on the previous elaborations, the following is expected: first, in general, the legitimacy strategies of digital surveillance technology are in line with existing privacy regimes, thus demonstrating that there are national trajectories and paths of legitimizing surveillance. This reasoning follows the idea that legacies of the past regarding privacy and surveillance management provide basic templates for current practices through path dependency (Steinmo et al., 1992). Second, the strategies are expected to be shaped by context-specific conditions related to overall crisis strategies in the COVID-19 pandemic.

Specifically, due to Germany's legacy of having a heavy privacy focus and privacy rule-following, it is expected that the government emphasizes compliance with privacy laws and adhering to IT standards, and that the influence of the overall crisis strategy – with a focus on rules and moral values – is not incongruent, but complementary to the legitimizing approach. Norway is also expected to emphasize privacy rule-following and IT standards, albeit not as much as Germany. In addition, the Norwegian government is expected to stress the cognitive dimension more than the other countries, by presenting the app as absolutely necessary to overcoming the crisis, in line with the communication in the overall crisis strategy. Relatedly, it is also expected that moral values such as "dugnad" are highlighted. The United Kingdom is expected to underline pragmatic legitimacy the most, with emphasis on self-interest and citizens' own health, due to its comparatively more flexible privacy regime, which opens for more importance of the overall crisis strategy. It is not expected that the UK will emphasize cognitive legitimacy, as the overall crisis measures were not presented as inevitable or

unequivocally intrusive and necessary. Overall, it is not claimed that the governments focus exclusively on one or the other, because in crisis situations governments might play all their cards, but it is expected that differences in ways of legitimizing can clearly be observed.

Method and data

The data consists of official press releases, press briefs, transcripts of government press conferences, question times and speeches, government reports, government blogs, statements on government websites, and news statements by politicians and experts communicating on behalf of the government. Throughout the pandemic, these were the main ways of communicating and justifying the crisis measures in the three countries. To obtain the data, the websites of the governments, the departments of health, health agencies, and relevant IT partners, which were the main actors involved in developing the technology, were thoroughly searched for all information related to the contact tracing apps. All three countries have a relatively transparent public sector, making relevant data easily accessible. An overview of the data sources is provided in Appendix A. The type of actors who communicated and legitimized the apps varied slightly between countries, but it mainly involved the prime minister, the minister of health, directors of the health authorities or other top administrative executives, and IT/health experts who were involved in developing the app. As some of the statements were archived or updated, Wayback Machine was used to retrieve original statements.

Collectively, these data sources give a comprehensive account of the rhetoric used to legitimize the digital surveillance technologies. The essential arguments and viewpoints that the governments embrace to justify their own decisions and get citizens to use the apps are contained in these sources. Consequently, because the main measures to handle the COVID-19 pandemic gained quite a lot of public attention, this data provides a rare opportunity to compare strategic legitimizing of the same digital surveillance technology between countries.

The data was analyzed using content analysis and the analysis was conducted in two stages. The first stage focused on identifying major themes and key communication actors within the data. In this stage, the range of beliefs, values, explanations, and justifications surrounding the apps was identified to ensure that the analysis encompassed the relevant communication and arguments, laying the foundation for the second stage.

The second stage of the analysis was concerned with categorizing and capturing the specific types of legitimacy. Here, the computer software NVivo was used to structure and systematize the data. A coding scheme was created for analyzing all the text segments that

contain the justification of choices and rhetoric to get citizens to use the contact tracing apps. All relevant text was coded based on the operationalization of the three dimensions in Table 1, which builds upon relevant literature (Suchman, 1995; Suddaby and Greenwood, 2005; Suddaby et al., 2017). This was done two times to ensure coding reliability. As shown in Appendix B, these statements ranged from a single sentence to longer paragraphs.

In such an analysis, statements will occasionally encompass more than one dimension of legitimacy. In those cases, statements were coded as multiple dimensions, but the most prominent one was emphasized. Sometimes, it was the case that the presence of another dimension corroborated the main standpoint, but it could also be its own argument.

Results

The results show that all three countries use several rhetorical strategies to legitimize their own choices and to influence citizens to support, accept, and use the app. However, variations can also clearly be observed. Table 3 provides an overview of the countries' approaches in legitimizing the digital surveillance technology in the COVID-19 pandemic. Furthermore, Appendix B provides a range of examples of statements and how they are coded in addition to those highlighted in the following.

First, Germany primarily embraced a moral strategy in legitimizing its app, the Corona-Warn-app[1], which concerned two overall aspects: protecting the community and highlighting normative values concerning transparency and IT-standards. Chancellor Angela Merkel, the leading face of Germany's crisis management, emphasized in her main speech about the app that:

> *Everyone who uses the app is helping to keep the virus under control, now and in the future… It was worthwhile insisting on absolute transparency, comprehensive data privacy, and the most rigorous IT security standards. Today we can say that the app deserves your trust. It protects your privacy since all data generated is encrypted, or pseudonomized, as the experts put it.*

The importance of standards and moral values is conveyed as a foundation for citizens to utilize the app in fighting the virus. What she tells next illustrates the dynamics between the moral approach and the pragmatic approach in Germany:

> *It is important to stress one thing, however, which is that using the app is entirely voluntary. There are no rewards for using it, and nobody will be penalized for not using*

[1] While Germany ended up also using another app, the Luca app, developed by private actors, this was launched substantially later in the pandemic, with different functions.

it. … It's obviously in our own interests to know if we have been exposed to the risk of infection. But the app also offers benefits for the community as a whole. And the more people who use the app, the greater the benefits. By acting sensibly and responsibly, together, we have contained the spread of the virus.

The communication is largely about creating and appealing to common moral values to guide and direct social behavior, without disregarding the benefits it also has for the individual. The German Chancellor was not the only one active in legitimizing the app. The Minister of Health Jens Spahn said that *"Every hour we gain by an early warning is a gain in our fight against this virus…»*, showing how the app can benefit the crisis management capacity of the government, with a focus on the community fighting the virus together.

Several German experts who were involved in developing the app were also involved in legitimizing the app. They tell much of the same story, reinforcing the importance of voluntary usage and benefits for society. They also emphasize how the app is complying with existing legislation about privacy, which data protection impact assessments were carried out, and the value of open source not only for transparency to increase the number of downloads, but also to illustrate regulatory compliance. Moreover, experts highlight how the Federal DPA was involved from the start in developing the app, and how they work to increase interoperability with apps in other EU countries, to increase crisis management capacity. These approaches contain both pragmatic and moral elements. There is little cognitive legitimizing from the German government. The only aspect that seems to be cognitively oriented is that one expert mentioned that the app is important because it can be superior to pen-and-paper methods in infection tracking. However, the same expert also highlights how the app is in no way a panacea.

Table 3. Overview of the apps, legitimacy strategies, and quotes in Germany, Norway, and the United Kingdom.

	Germany	**Norway**	**United Kingdom**
App name and organizations involved in development	Corona-Warn-App (developed by Robert Koch Institute, SAP, and Deutsche Telekom).	Smittestopp (developed by Norwegian Institute of Public Health and the public research institute Simula).	NHS COVID-19 (developed by the National Health Service and company VMware).
Main emphasis in legitimizing the digital surveillance technology in the COVID-19 pandemic	Main: Moral legitimizing (protecting community and IT standards). Also stress rule-following and compliance.	Main: Pragmatic legitimizing (increasing crisis management capacity). Also, cognitive legitimizing and some focus on moral values.	Main: Pragmatic legitimizing (self-interest – citizens' benefits), and regulatory compliance. Also, non-cognitive approach.

Representative quotes	"I don't know anything about you, but I'll protect you." (Slogan when the app was launched).	"Smittestopp is an app that is connected to several other things we want to do, such as … follow and study the development and impact of the [other] measures. It is absolutely crucial to be able to stop measures that harm society and that are difficult to live with over time."	"Gran doesn't need the app to benefit from it. If you download the app, you're protected and you're more likely to be protecting the people you care about around you."

The Norwegian government legitimized its app somewhat differently compared to Germany. First, the pragmatic approach in Norway was more about the government and the Norwegian Institute of Public Health (NIPH) increasing their infection tracking capacity, and how the app provides data about the movements of groups in society to measure the effect of other crisis measures to deal with the spread of the virus. The NIPH highlighted that the app would have immediate utility in assessing other crisis measures, and utility for individual citizens when they get notifications from being in contact with infected persons. Moreover, the NIPH highlighted that infection tracking is done manually in the municipalities which is time-consuming. The Minister of Health endorsed this pragmatic-cognitive approach by stating that:

> *Today's technology gives us the opportunity that no one has had before to prevent infection, disease, and death. We must dare to adopt new technology and develop new methods, but it can be demanding.*

The minister highlights the technological superiority that digital contact tracing can have in solving current problems society faces, and challenges old ideas about technology at a cognitive level. Specific rule-following was not much highlighted in Norway, but involved IT experts pointed out that "*well-established industry and encryption standards are used to secure the app*". In her call to get people to use the app, Prime Minister Erna Solberg said that *"if we want more freedom faster, this is the way to go"* and *"if we are to get our everyday life back, as many people as possible should download the app".* Here, the technology is presented as a fundamental prerequisite to overcoming the major crisis and to "reclaim" basic social values and a sense of "normality". It is an attempt to influence collective meaning for how citizens are to interpret and respond to the situation of great threat and uncertainty. The Prime Minister also

said that downloading the app is a continuation of the "dugnad", meaning voluntary community work, that all Norwegian citizens were already involved in.

The app in Norway was eventually deactivated, due to a combination of privacy concerns and low infection numbers (Lund-Tønnesen, 2022). As a response to this, the director of the NIPH said that "*we are dependent on legitimacy*", and that with the ban "*we weaken an important part of our preparedness against the increased spread of infection*". Additionally, the director stressed how the app is about enhancing capacity in crisis management, but she does not bring up other advantages (e.g., for citizens):

> *The pandemic is not over. We have no immunity in the population, no vaccine, and no effective treatment. Without the Smittestopp app, we will be less equipped to prevent outbreaks that may occur locally or nationally.*

Furthermore, the United Kingdom focuses much on pragmatic legitimacy. This concerns both how citizens are encouraged to utilize the app, but also the government's adherence to privacy regulations in designing the technology. The encouragement to download the app was largely based on citizens' own interests. The emphasis was on citizens' own assessments and benefits for the health of themselves or someone close to them, and not for unknown others, although the community and nation-state are occasionally mentioned. In a major TV campaign, the government advertised extensively with the slogan: "*Protect your loved ones. Get the app*". Moreover, when launching the pilot version of the app, the NHSX chief executive Matt Gould said that "*the app will give the public a simple way to make a difference and to help keep themselves and their families safe*". In the same regard, health secretary Matt Hancock said that by downloading the app "*you are protecting your own health, you are protecting the health of your loved ones and the health of your community*".

Moreover, the UK government communicated frequently how the app is compliant with UK GDPR and highlighted it as "*ultra-secure*". In the same regard, they occasionally highlight transparency and standards of privacy related to the app, and that any changes would be explained in "plain English". Furthermore, as the app encountered technical problems and was opposed by many, the health secretary backtracked the previously stated importance of the app, and rather embraced the opposite of a cognitive approach when he stated that it was better to *"get confidence that people are following the advice that's given by human beings before introducing the technological element".* Prime Minister Boris Johnson, who was not much involved in legitimizing the app, supported this by saying that the contact tracing app was not a crucial part of contact tracing work but rather the "*icing on the cake*". Overall, the UK

government's legitimacy strategy had a main emphasis on citizens' own assessments but also involved some of the other legitimacy aspects.

Discussion

A major challenge in managing the COVID-19 pandemic was that governments were required to balance different kinds of values such as public health and safety towards individual liberty and privacy (Boin and Lodge, 2021b). Due to the urgency of the pandemic and the limited knowledge regarding the coronavirus' clinical-epidemiological features, the potential consequences of different alternatives for crisis measures and digital surveillance technologies were not sufficiently evaluated by any government (Hu and Liu, 2022). Interestingly, Germany spent some more time developing its app than the other countries, which seemed to pay off. In fact, among the three studied countries, only Germany ended up with a widely used multi-purpose app throughout the pandemic. Although the Norwegian government perceived that it had leeway to implement an intrusive surveillance technology, in reality, this was not the case, which became evident when the app was banned by the Norwegian DPA (Lund-Tønnesen, 2022). Relatedly, the UK ended up delaying its app for many months.

In Norway and the UK, the apps were launched slightly quicker than in Germany, but still after the initial critical lockdown measures that many governments around the world implemented. It is noteworthy that this particular measure at times received more negative media attention compared with other rushed measures with potentially much more detrimental repercussions for individuals and society, both short-term and long-term (Villius Zetterholm et al., 2021). These potential repercussions are evident in the Norwegian case, where several central decision-makers admitted that some of the lockdown measures were too strict for children and young people and with their current knowledge they would not have implemented those measures (Lund-Tønnesen and Christensen, 2023b). The negativity surrounding surveillance may be because of its unclear purposes. Although they are said to be in line with the GDPR, the purposes may still be unclear for citizens, which is a common phenomenon when implementing surveillance (Trüdinger and Steckermeier, 2017). Therefore, we can think that legitimizing a controversial policy such as those involving surveillance is particularly important for governments when the policy is ambiguous, and the situation and problem are also rather ambiguous (Christensen and Lægreid, 2022). However, even if many of the challenges of major crises are similar across countries, the governmental responses are dependent on country-specific conditions (Kuhlmann et al., 2021).

Going back to the theoretical assumptions based on path dependency, we can use this construct to interpret several aspects of the main results regarding surveillance legitimizing. A main finding is that Germany extensively stresses moral values for using the technology and compliance with privacy rules. This can be understood based on the country's legacy of taking privacy issues very seriously, which stems from privacy being ingrained in German culture and in established legal-administrative principles that have rule-following at their core (Bygrave, 2004). This backdrop makes it near unthinkable to deviate from existing regulations in developing important technologies, even to improve own crisis management capacity.

Norway has a history of protecting privacy but also perceived leeway for the government to utilize surveillance when combating extensive societal problems (Rykkja et al., 2011), which can help us understand why some privacy concerns are given less importance by the government when surveillance is asserted to be inevitable for returning to "normality" and for improving crisis management capacity. In such a manner, the Norwegian government's approaches to dealing with privacy and surveillance come across as relatively path-dependent.

In the UK, the self-interest aspect of the pragmatic dimension is considerably more highlighted than in the other countries. This reflects the overall crisis approach at the time, which stressed that citizens must do their own assessments. Somewhat surprisingly, the UK also focused much on rule-following and regulatory compliance, which was not expected based on the assumptions about path dependency. One possible explanation for this is that because the government did not communicate a sense of urgency or uncertainty about the pandemic at this early stage, the cards it could play to legitimize the app were limited.

Overall, Germany emphasizes values and justifications precisely in accordance with what one would expect from a country with a history of strict and extensive rules of privacy. Moreover, because governments in Norway and the UK have less of a tradition of being overly strict with regards to privacy matters and have some perceived leeway in utilizing digital technology that includes the collection and use of personal data about citizens, they stress these matters less and focus on other aspects. Path dependency thus demonstrates explanatory power in this policy area and is a valuable construct in understanding how history matters for surveillance legitimizing. Yet, privacy legacies alone do not shape all of the legitimacy aspects that are embraced, and the overarching crisis strategy must also be taken into account (Christensen and Lægreid, 2020). In Norway, the crisis strategy is important, and the legitimizing reflects the approach of stressing cognitive beliefs. In the UK, the crisis strategy seems to complement the privacy legacy where the regime is more flexible. Germany's crisis

strategy based on moral values and semi-lockdown seems to be in accordance with its privacy regime. In this way, we need to supplement the path dependency interpretations by also viewing the pandemic as a unique situation that involves strategies that depart from existing trajectories. We can view the COVID-19 pandemic as a key point in the evolution of government surveillance and think that it is a critical juncture that might determine new, but also reinforce old pathways and directions for institutional development and changes in privacy regimes and legacies.

The classification of different types of legitimacy strategies developed in this study provides an important way of understanding legitimacy rhetoric and argumentation patterns about surveillance. Consistent with the observations of extant research, institutional conditions and established practices are important for the different ways these strategies take (Pauli et al., 2016; Ochoa et al., 2021; Villar and Magnawa, 2022). In this study, we can think that the experiences from the pandemic have meant that e.g., in Norway, there is now less perceived leeway than before the pandemic, and that this crisis functions as a critical juncture and an adjustment of practices in the historical development of the privacy regime. By a similar token, we can expect the German government to perceive the leeway as it already does, and that the experiences from the pandemic are reinforcing existing practices.

Viewing these findings and conditions in relation to the mega-trend of digitalization and emerging technologies such as artificial intelligence, we can expect higher uncertainty and frequent changes in expectations, norms, values, and ideologies in public administrations' institutional environment and fewer calm periods of adaptions than before (Fossheim and Lund-Tønnesen, 2023). The challenges of legitimizing future digital surveillance technologies and their impact on the public administrative apparatus are likely not so much about the technical aspects themselves, but the inconsistent political, social, and moral values and expectations that they bring with them (Ahn and Chen, 2022; Fossheim and Lund-Tønnesen, 2023), combined with the uncertain crisis conditions in which many surveillance measures are introduced (Boersma and Fonio, 2018; Villar and Magnawa, 2022). Digital contact tracing apps are a prime example of this.

Dealing with these changing values and expectations seems to be an increasingly precarious endeavor for public administrations, yet one that some believe surveillance could assist in by providing data to improve decision-making. However, more digital surveillance technology means more personal data, which generates more demand for secure systems that protect that data from adversaries, unintended use, and data leaks (Boersma and Fonio, 2018).

This gives rise to demands for legitimate systems of surveillance. If legitimacy is high, governments might obtain slack to implement more surveillance technologies (Lund-Tønnesen and Christensen, 2023a). However, this can also lead to a complicated development where some surveillance technologies of some organizations are more legitimate and utilized than others, thereby increasing complexity in the public administrative system and in the public organizations that have personal data as a core part of their problem-solving functions, such as tax, welfare and health administrations, national security organizations and the police.

Conclusion

Overall, the study finds that the governments in Germany, Norway, and the United Kingdom legitimize their digital contact tracing apps in both similar and different ways. These approaches – involving pragmatic, moral, and cognitive strategies – are in line with the three countries' respective privacy regimes and legacies, as well as their overall crisis strategies employed to combat the COVID-19 pandemic (Bennett and Raab, 2006; Christensen and Lægreid, 2020). Path dependency plausibly explains much of the approaches to legitimizing the digital surveillance technology in the three countries, demonstrating how privacy arrangements and practices are shaped historically. This indicates that legitimizing operates within this institutional setting of potential conduct, but the study also shows how the current context, the pandemic in this case, matters for the legitimizing strategies.

Despite presumptions of equivalent surveillance and privacy approaches grounded in a common EU framework for data protection regulation, the findings show how historical legacies to privacy still shape countries' practices today. This has added value to the study of the politics of surveillance and privacy in times of crisis, and the study of surveillance legitimacy, beyond the one tool examined in this study. By focusing on the underexplored aspect of how and under what conditions the legitimacy of surveillance is gained and created, the study also contributes to the literature on legitimizing surveillance (e.g., Schulze, 2015; Tiainen, 2017; Kuehn, 2018). Importantly, it also demonstrates that we need to understand the implementation of digital surveillance technology in crisis management not only as a matter of governance capacity but also governance legitimacy (Christensen et al., 2016).

An important lesson when interpreting the legitimizing approaches is that there is in some cases partial overlap between the influence of privacy regime legacies and the overall crisis strategies. That makes it difficult to know which of these factors matters most. However, it corroborates the idea that context matters for legitimizing surveillance. Because context matters, we need to keep that in mind when viewing the findings from this study in comparison

with other countries. The analytical way of viewing legitimacy strategies developed in this study, by focusing on pragmatic, moral, and cognitive legitimacy, will be applicable in other countries as well. However, the actual outcomes of the strategies are expected to vary, just as in the three studied countries. Variations might be greater in other regions, as the three countries in this study are all situated in Europe, a region where privacy regulations have in the last fifty years been generally stricter (Bennett and Raab, 2006).

An expected development in the digital age is that surveillance becomes more ubiquitous (Yates and Whitford, 2022). That can lead to more demands for transparency from citizens and regulators. In future crises, even if these situations are deemed exceptional, governments may need to provide more clarity about technicalities, intended goals, and duration of surveillance in order to gain and maintain legitimacy. These demands will likely vary between different technologies. Future research should investigate the legitimizing of other digital surveillance technologies, for example those that involve artificial intelligence, machine learning, and big data, and advance the comparative work on the significance of privacy regimes and situations involving uncertainty and complexity which this study has only begun to explore.

Literature

Ahn, M. J. and Chen, Y.-C. 2022. Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government. *Government Information Quarterly,* 39**,** 101664.

Arora, S., Debesay, J. and Eslen-Ziya, H. 2022. Persuasive narrative during the COVID-19 pandemic: Norwegian Prime Minister Erna Solberg's posts on Facebook. *Humanities and Social Sciences Communications,* 9**,** 1-10.

Beasley, V. B. 2011. *You, the people: American national identity in presidential rhetoric*, Texas A&M University Press.

Bellamy, C., 6, P. and Raab, C. 2005. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. *Public Administration,* 83**,** 393-415.

Bennett, C. and Raab, C. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edn. MIT Press, Cambridge, MA.

Boersma, K. and Fonio, C. 2018. Big data, surveillance and crisis management. *Big data, surveillance and crisis management.* Routledge.

Boersma, K., Van Brakel, R., Fonio, C. and Wagenaar, P. 2014. *Histories of state surveillance in Europe and beyond*, Routledge.

Boin, A. and Lodge, M. 2016. Designing resilient institutions for transboundary crisis management: A time for public administration. *Public administration,* 94**,** 289-298.

Boin, A. and Lodge, M. 2021a. Responding to the COVID-19 crisis: a principled or pragmatist approach? *Journal of European Public Policy***,** 1-22.

Boin, A. and Lodge, M. 2021b. Responding to the COVID-19 crisis: a principled or pragmatist approach? *Journal of European Public Policy,* 28**,** 1131-1152.

Boin, A., T Hart, P., Stern, E. and Sundelius, B. 2005. *The Politics of Crisis Management – Public Leadership Under Pressure*. Cambridge: Cambridge University Press.

Boin, C., Lodge, M. and Shields, H. 2023. The Sick Man of Europe: The United Kingdom's COVID-19 Response. *Crisis Leadership and Public Governance during the COVID-19 Pandemic: International Comparisons.*

Bygrave, L. A. 2004. Privacy protection in a global context–a comparative overview. *Scandinavian Studies in Law,* 47**,** 319-348.

Christensen, T. and Lægreid, P. 2020. The coronavirus crisis—crisis communication, meaning-making, and reputation management. *International Public Management Journal,* 23**,** 713-729.

Christensen, T. and Lægreid, P. 2022. Scientization under pressure—The problematic role of expert bodies during the handling of the COVID-19 pandemic. *Public Organization Review,* 22**,** 291-307.

Christensen, T., Lægreid, P. and Rykkja, L. H. 2016. Organizing for Crisis Management: Building Governance Capacity and Legitimacy. *Public administration review,* 76**,** 887-897.

Davis, D. W. and Silver, B. D. 2004. Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American journal of political science,* 48**,** 28-46.

Degli Esposti, S., Ball, K. and Dibb, S. 2021. What's in it for us? Benevolence, national security, and digital surveillance. *Public Administration Review,* 81**,** 862-873.

Flaherty, D. 1989. *Protecting privacy in surveillance socities: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill (NC): University of North Carolina Press.

Fossheim, K. and Lund-Tønnesen, J. 2023. Digitalization of public sector organizations over time: The applicability of quantitative text analysis. *International Review of Administrative Sciences***,** 00208523231183569.

Hammerschmid, G., Palaric, E., Rackwitz, M. and Wegrich, K. 2023. A shift in paradigm? Collaborative public administration in the context of national digitalization strategies. *Governance*.

Hart, R. P., Daughton, S. M. and Lavally, R. 2005. Modern rhetorical criticism.

Hu, Q. and Liu, Y. 2022. Crisis management and national responses to COVID-19: Global perspectives. *Public Performance & Management Review,* 45**,** 737-750.

Krasner, S. D. 1988. Sovereignty: An Institutional Perspective. *Comparative Political Studies,* 21**,** 66-94.

Kuehn, K. M. 2018. Framing mass surveillance: Analyzing New Zealand's media coverage of the early Snowden files. *Journalism,* 19**,** 402-419.

Kuhlmann, S., Franzke, J. and Dumas, B. P. 2022. Technocratic Decision-Making in Times of Crisis? The Use of Data for Scientific Policy Advice in Germany's COVID-19 Management. *Public Organization Review,* 22**,** 269-289.

Kuhlmann, S., Hellström, M., Ramberg, U. and Reiter, R. 2021. Tracing divergence in crisis governance: responses to the COVID-19 pandemic in France, Germany and Sweden compared. *International Review of Administrative Sciences,* 87**,** 556-575.

Kuhlmann, S. and Wollmann, H. 2019. *Introduction to comparative public administration: Administrative systems and reforms in Europe*, Edward Elgar Publishing.

Lischka, J. A. 2017. Explicit terror prevention versus vague civil liberty: How the UK broadcasting news (de) legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society,* 20**,** 665-682.

Lund-Tønnesen, J. 2022. Regulating emerging technology in times of crisis: Digital contact tracing in Norway during the Covid-19 pandemic. *Law & Policy,* 44**,** 278-298.

Lund-Tønnesen, J. and Christensen, T. 2023a. The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic. *International Public Management Journal,* 26**,** 126-144.

Lund-Tønnesen, J. and Christensen, T. 2023b. Learning from the COVID-19 Pandemic: Implications from Governance Capacity and Legitimacy. *Public Organization Review*.

Lægreid, P. and Rykkja, L. H. 2023. Strategic public management in crises. *Handbook on Strategic Public Management.* Edward Elgar Publishing.

Ochoa, C. S., Gadinger, F. and Yildiz, T. 2021. Surveillance under dispute: Conceptualising narrative legitimation politics. *European Journal of International Security,* 6**,** 210-232.

Pauli, R., Sarwary, H., Imbusch, P. and Lukas, T. 2016. "Accepting the Rules of the Game": Institutional Rhetorics in Legitimizing Surveillance. *European Journal for Security Research,* 1**,** 115-133.

Pierson, P. 2000. Increasing returns, path dependence, and the study of politics. *American political science review,* 94**,** 251-267.

Reyes, A. 2011. Strategies of legitimization in political discourse: From words to actions. *Discourse & society,* 22**,** 781-807.

Rykkja, L. H., Lægreid, P. and Lise Fimreite, A. 2011. Attitudes towards anti-terror measures: The role of trust, political orientation and civil liberties support. *Critical Studies on Terrorism,* 4**,** 219-237.

Schulze, M. 2015. Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society,* 13**,** 197-217.

Scott, W. R. 2014. *Institutions and organizations : ideas, interests, and identities,* Thousand Oaks, Calif, Sage.

Steinmo, S. 2008. Historical institutionalism. *Approaches and methodologies in the social sciences: A pluralist perspective***,** 118-138.

Steinmo, S., Thelen, K. and Longstreth, F. 1992. *Structuring politics: historical institutionalism in comparative analysis*, Cambridge University Press.

Suchman, M. C. 1995. Managing legitimacy: Strategic and institutional approaches. *Academy of management review,* 20**,** 571-610.

Suddaby, R., Bitektine, A. and Haack, P. 2017. Legitimacy. *Academy of Management Annals,* 11**,** 451-478.

Suddaby, R. and Greenwood, R. 2005. Rhetorical strategies of legitimacy. *Administrative science quarterly,* 50**,** 35-67.

Svenbro, M. and Wester, M. 2023. Examining Legitimacy in Government Agencies' Crisis Communication. *International Journal of Strategic Communication,* 17**,** 54-73.

Tiainen, M. 2017. (De) legitimating electronic surveillance: A critical discourse analysis of the Finnish news coverage of the Edward Snowden revelations. *Critical Discourse Studies,* 14**,** 402-419.

Trüdinger, E.-M. and Steckermeier, L. C. 2017. Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly,* 34**,** 421-433.

Van Leeuwen, T. 2007. Legitimation in discourse and communication. *Discourse & communication,* 1**,** 91-112.

Versluis, E. 2007. Even rules, uneven practices: Opening the 'black box'of EU law in action. *West European Politics,* 30**,** 50-67.

Villar, E. B. and Magnawa, J. P. 2022. Surveillance and pandemic governance in least-ideal contexts: The Philippine case. *Journal of Contingencies and Crisis Management,* 30**,** 22-31.

Villius Zetterholm, M., Lin, Y. and Jokela, P. Digital contact tracing applications during COVID-19: a scoping review about public acceptance. Informatics, 2021. MDPI, 48.

Wahl-Jorgensen, K., Bennett, L. and Taylor, G. 2017. The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication,* 11**,** 740-762.

Whitman, J. Q. 2004. The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal***,** 1151-1221.

Yates, J. and Whitford, A. B. 2022. Surveillance as the Past and Future of Public Administration. *Perspectives on Public Management and Governance.*

Yeung, K. and Bygrave, L. A. 2022. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance,* 16**,** 137-155.

Appendix A: Overview of data sources.

BBC. 2020. NHS Covid-19 app: One million downloads of contact tracer for England and Wales. BBC. Retrieved 5 April 2023. https://www.bbc.com/news/technology-54270334

Bishop's Stortford. 2020. The NHS COVID-19 app - protecting our loved ones from coronavirus. Produced in association with the UK government. Retrieved 3 April 2023. https://www.bishopsstortfordindependent.co.uk/news/the-fastest-way-of-knowing-when-youre-at-risk-from-coronavirus-9127029/

Bundesregierung. 2020a. The more people who use the app, the greater the benefits. German government. Retrieved 20 March 2023. https://www.bundesregierung.de/breg-de/service/archiv/archiv-mediathek/the-more-people-who-use-the-app-the-greater-the-benefits-1763140

Bundesregierung. 2020b. People want it, it works, it is helping. German government. Retrieved 20 March 2023. https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-warn-app-1790632

Bundesregierung. 2020c. How does the Corona-Warn-App work and what does it do?. German government. Retrieved 23 March. https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch/how-does-the-corona-warn-app-work-and-what-does-it-do--1758870

Bundesregierung. 2020d. Die wichtigsten Fragen und Antworten. German government. Retrieved 23 March 2023. https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392

Channel4. 2020. Boris Johnson repeats claim that no country has a functioning Covid-19 tracing app. Channel4. Retrieved 5 April 2023 https://www.channel4.com/news/factcheck/factcheck-boris-johnson-repeats-claim-that-no-country-has-a-functioning-covid-19-tracing-app

Corona warn-app open source project. 2020a. Help us improve the Corona-warn-app. German government. Retrieved 23 March 2023. https://www.coronawarn.app/en/

Corona warn-app open source project. 2020b. Blog. German government. Retrieved 24 March 2023. https://www.coronawarn.app/en/blog/

Corona warn-app open source project. 2020c. News archive. German government. Retried 29 March 2023. https://www.coronawarn.app/en/blog/archive/

Department of Health and Social Care. 2020a. NHS COVID-19 app compatible with contact tracing apps across UK, Jersey and Gibraltar. UK Government. Retrieved 4 April 2023. https://healthtech.blog.gov.uk/2020/11/05/nhs-covid-19-app-compatible-with-contact-tracing-apps-across-uk-jersey-and-gibraltar/

Department of Health and Social Care. 2020b. How the NHS COVID-19 app is making the most of cutting-edge global technology. UK Government. Retrieved 4 April 2023. https://healthtech.blog.gov.uk/2020/10/29/how-the-nhs-covid-19-app-is-making-the-most-of-cutting-edge-global-technology/

Department of Health and Social Care. 2020c. NHS COVID-19 app launches across England and Wales. UK Government. Retrieved 5 April 2023. https://www.gov.uk/government/news/nhs-covid-19-app-launches-across-england-and-wales

Deutsche Telekom. 2020a. #CoronaWarnApp – der digitale Virus-Wachhund – Folge 4. Telekom. Retrieved 27 March 2023. https://www.youtube.com/watch?v=mA5X10SCznY

Deutsche Telekom. 2020b. #CoronaWarnApp – der digitale Virus-Wachhund – Folge 5 Telekom. Retrieved 27 March 2023 https://www.youtube.com/watch?v=jhQ3Vbx-ELI

Deutsche Telekom. 2020c. #CoronaWarnApp – der digitale Virus-Wachhund – Folge 7 Telekom. Retrieved 27 March 2023 https://www.youtube.com/watch?v=SNiNQLPry2A

Deutsche Telekom 2020d. Datenschutz schafft Vertrauen für Corona-Warn-App. Deutsche Telekom. Retrieved 29 March 2023 https://www.telekom.com/de/konzern/details/datenschutz-schafft-vertrauen-fuer-corona-warn-app-600522

Deutsche Telekom 2020e. Demokratie und Digitalisierung brauchen einander Deutsche Telekom. Retrieved 29 March 2023. https://www.telekom.com/de/konzern/management-zur-sache/details/demokratie-und-digitalisierung-brauchen-einander-601088

Digileaders. 2020. The power of data in a pandemic. Post by NHS. Retrieved 3 April 2023. https://digileaders.com/the-power-of-data-in-a-pandemic/

Digitalhealth. 2020a. Timeline: What happened with the NHS Covid-19 app. Digitalhealth. Retrieved 3 April 2023. https://www.digitalhealth.net/2020/04/timeline-what-happened-with-the-nhs-covid-19-app/

Digitalhealth. 2020b. NHS coronavirus contact-tracing app ‘delayed until June’. Digitalhealth. Retrieved 5 April 2023. https://www.digitalhealth.net/2020/05/nhs-coronavirus-contact-tracing-app-delayed-until-june/

Euractiv. 2020. German government presents ‘best coronavirus tracing app worldwide’. Euractiv. Retrieved 20 May 2023 https://www.euractiv.com/section/digital/news/german-government-presents-best-coronavirus-tracing-app-worldwide/

Independent. 2020. Coronavirus: NHS contact-tracing app may not be ready until winter, health minister admits. Independent. Retrieved 5 April 2023. https://www.independent.co.uk/news/uk/politics/coronavirus-contract-tracing-app-uk-nhs-a9571461.html

The Guardian. 2020a. Germany appeals to nation to download coronavirus app. The Guardian. Retrieved 23 March 2023. https://www.theguardian.com/world/2020/jun/16/germany-appeals-to-nation-to-download-coronavirus-app

The Guardian. 2020b. UK abandons contact-tracing app for Apple and Google model. The Guardian. Retrieved 5 April 2023. https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models

LGA. 2020. LGA responds to launch of NHS COVID-19 app. Local Government Association. Retrieved 4 April 2023. https://www.local.gov.uk/about/news/lga-responds-launch-nhs-covid-19-app

Linkedin. 2020a. Corona-Warn-App: Wo stehen wir nach dem ersten Monat?/ The First Month in Review. Linkedin Retrieved 27 March 2023. https://www.linkedin.com/pulse/corona-warn-app-wo-stehen-wir-nach-dem-ersten-monat-first-mueller

Linkedin, 2020b. Corona-Warn-App: Und sie funktioniert doch! / It really does work!. Linkedin. Retrieved 27 March 2023. https://www.linkedin.com/pulse/corona-warn-app-und-sie-funktioniert-doch-juergen-mueller

Nettavisen. 2020. Erna Solberg and Bent Høie defend the Smittestopp app. Nettavisen. Retrieved 11 April 2023. https://www.nettavisen.no/nyheter/erna-solberg-og-bent-hoie-forsvarer-smittestopp-appen/s/12-95-3423982380

NIPH. 2020a. Updates about the work with new Smittestopp. Norwegian Institute of Public Health. Retrieved 29 March 2023. https://www.fhi.no/historisk-arkiv/covid-19/smittestopp/digital_smittesporing/

NIPH. 2020b. Smittestopp – historical archive. Norwegian Institute of Public Health. Retrieved 29 March 2023. https://www.fhi.no/historisk-arkiv/covid-19/smittestopp/

NIPH. 2020c. The technology behind Smittestopp. Norwegian Institute of Public Health. Retrieved 30 March 2023. https://www.fhi.no/historisk-arkiv/covid-19/smittestopp/lagringsteknologi/

NIPH. 2020d. Digital contact infection tracing with Smittestopp 16 April 2020. Norwegian Institute of Public Health. Retrieved 3 April 2023. https://www.fhi.no/historisk-arkiv/artikler/smittestopp/slik-har-fhi-utviklet-smittestopp/

NIPH. 2020e. Drammen, Tromsø and Trondheim tests notification with Smittestopp. Norwegian Institute of Public Health. Retrieved 3 April 2023. www.fhi.no/nyheter/2020/drammen-tromso-og-trondheim-tester-varsling-med-smittestopp

NIPH. 2020f. We need more Smittestopp users - 7 May 2020. Norwegian Institute of Public Health. Retrieved 3 April 2023. https://www.fhi.no/nyheter/2020/vi-trenger-flere-smittestopp-brukere

NIPH. 2020g. Notified decision from the Norwegian Data Protection Authority. Norwegian Institute of Public Health. Retrieved 3 April 2023. https://www.fhi.no/nyheter/2020/varsel-om-vedtak-om-palegg-fra-datatilsynet/

NIPH. 2020h. the NIPH has received the report from the expert group about Smittestopp. Norwegian Institute of Public Health. Retrieved 3 April 2023. https://www.fhi.no/nyheter/2020/fhi-har-mottatt-rapport-fra-ekspertgruppen-om-smittestopp/

NIPH. 2020i. The NIPH stops all data collection in Smittestopp. Norwegian Institute of Public Health. Retrieved 3 April 2023. https://www.fhi.no/nyheter/2020/fhi-stopper-all-innsamling-av-data-i-smittestopp/

NHS. 2020a. Regulating AI in health and care. UK NHS. Retrieved 4 April 2023. https://digital.nhs.uk/blog/transformation-blog/2020/regulating-ai-in-health-and-care

NHS. 2020b. Digital contact tracing: protecting the NHS and saving lives. UK NHS. Retrieved 4 April 2023. https://transform.england.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/

NHS. 2020c. How technology helped shape the pandemic response. UK NHS. Retrieved 4 April 2023. https://transform.england.nhs.uk/blogs/how-technology-helped-shape-pandemic-response/

NHS. 2020d. NHS COVID-19 app now compatible across whole of UK, Jersey and Gibraltar. Welsh Government. Retrieved 5 April 2023. https://www.gov.wales/nhs-covid-19-app-now-compatible-across-whole-uk-jersey-and-gibraltar

Norwegian Government. 2020a. Press conference about better virus tracing and increased testing of the coronavirus 16 April 2020. Norwegian Government. Retrieved 29 March 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/smk/pressemeldinger/2020/pressekonferanse-om-bedre-smittesporing-og-okt-testing-av-koronavirus/id2697729/

Norwegian Government. 2020b. Dare to adopt new methods. 20 May 2020. Norwegian Government (Speech Minister of Health). Retrieved 29 March 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/hod/taler-og-innlegg/minister/taler-av-helse-og-omsorgsminister-bent-/2020/torre-a-ta-i-bruk-nye-metoder/id2703491/

Norwegian Government 2020c. The meter must not be shortened. 17 June 2020. Norwegian Government (Speech Minister of Health). Retrieved 29 March 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/hod/taler-og-innlegg/minister/taler-av-helse-og-omsorgsminister-bent-/2020/meteren-ma-ikke-krympe/id2714499/

Norwegian Government 2020d. Statement on the corona pandemic. (Minister of Health's presentation before the Storting). Retrieved 29 March 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/hod/taler-og-innlegg/minister/taler-av-helse-og-omsorgsminister-bent-/2020/redegjorelse-om-koronapandemien-i-stortinget/id2770148/

Norwegian Government. 2020e. Expert group proposes improvements in the Smittestopp app 20 May 2020. Norwegian Government. Retrieved 3 April 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/hod/nyheter/2020ny/ekspertgruppe-foreslar-forbedringer-i-smittestopp-appen/id2703470/

Norwegian Government. 2020f. The way forward for digital infection tracing. Norwegian Government (Speech Minister of Health). Retrieved 11 April 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/hod/taler-og-innlegg/minister/taler-av-helse-og-omsorgsminister-bent-/2020/digital-smittesporing/id2766409/

Norwegian Government. 2020g. The corona situation: Press conference with the Minister of Health Monday 21. December. Norwegian Government. Retrieved 11 April 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-

solberg/hod/nyheter/2020ny/koronasituasjonen-pressekonferanse-med-helse-og-omsorgsministeren-mandag-21.-desember-2020/id2815230/

Norwegian Ministry of Justice and Preparedness. 2020a. Press conference about the corona situation 21. April 2020. Norwegian Government. Retrieved 29 March 2023. https://www.facebook.com/watch/live/?ref=watch_permalink&v=160893978610440

Norwegian Ministry of Justice and Preparedness. 2020b. The corona situation: press conference with the Minister of Justice and Minister of Health 20 May 2020. Norwegian Government. Retrieved 3 April 2023. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/jd/pressemeldinger/2020/koronasituasjonen-pressekonferanse-med-justisministeren-og-helseministeren3/id2703348/

NRK. 2020. Solberg: If we want more freedom faster – then this is the way to go. Norwegian Broadcasting Corporation. Retrieved 11 April 2023. https://www.nrk.no/norge/solberg_-_-om-vi-vil-ha-meir-fridom-raskare-_-da-er-dette-vegen-a-ga-1.14984882

SAP. 2020a. Corona-Warn-App Entwicklung: Von der Uni in die Königsklasse. SAP. Retrieved 27 March 2023. https://news.sap.com/germany/2020/07/corona-warn-app-entwicklung-universitaet/

SAP. 2020b. Corona-Warn-App-Entwicklung: „Bug-Fixing“ mit Sorgfalt. SAP. Retrieved 27 March 2023. https://news.sap.com/germany/2020/08/corona-warn-app-bug-fixing/

SAP. 2020c. Die populärsten Irrtümer zur Corona-Warn-App. SAP. Retrieved 29 March 2023. https://news.sap.com/germany/2020/06/fakten-corona-warn-app/

SAP. 2020d. In knapp 50 Tagen programmiert: Telekom und SAP veröffentlichen Corona-Warn-App. SAP. Retrieved 29 March 2023. https://news.sap.com/germany/2020/06/veroeffentlichung-corona-warn-app/

SAP. 2020e. Corona-Warn-App Entwicklung: „Wir befinden uns in der heißen Phase“. SAP. Retrieved 29 March 2023. https://news.sap.com/germany/2020/06/corona-warn-app-letzte-tests/

SAP. 2020f. Corona-Warn-App Entwicklung: “Publish often and early”. SAP. Retrieved 29 March 2023. https://news.sap.com/germany/2020/05/corona-warn-app-entwicklung-axel-sturm/

Solberg, Erna. 2020. If many people download Smittestopp. Post on Facebook. Retrieved 11 April 2023. https://www.facebook.com/ernasolberg/posts/hvis-mange-laster-ned-smittestopp-kan-vi-sammen-forkorte-perioden-med-inngripend/10158047529911832/

The Telegraph. 2020. Matt Hancock explains NHS Test, Track, Trace app launching on Isle of Wight. The Telegraph. Retrieved 4 April 2023. https://www.youtube.com/watch?v=AmQdA03Rj1k

UK Government. 2020. Guidance [Withdrawn] NHS COVID-19 app: how the app works. UK Government. Retrieved 4 April 2023. https://www.gov.uk/government/publications/nhs-covid-19-app-user-guide/nhs-covid-19-app-how-the-app-works

UK Health Security Agency. 2020. Guidance [Withdrawn] NHS COVID-19 app: privacy notice. UK Health Security Agency. Retrieved 4 April 2023.

https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice

UK Parliament. 2020a. Prime Minister's Questions: 20 May 2020. UK Parliament. Retrieved 3 April 2023. https://www.youtube.com/watch?v=SEkxDvV8pog

UK Parliament. 2020b. Prime Minister's Questions: 3 June 2020. UK Parliament. Retrieved 3 April 2023 https://www.youtube.com/watch?v=K7_okc3JLJY

UK Parliament. 2020c. Prime Minister's Questions: 10 June 2020. UK Parliament Retrieved 3 April 2023 https://www.youtube.com/watch?v=YU2XHd8k_jU

UK Parliament. 2020d Prime Minister's Questions: 17 June 2020. UK Parliament Retrieved 3 April 2023. https://www.youtube.com/watch?v=v0adyAfIhG8

UK Parliament. 2020e. Prime Minister's Questions: 24 June 2020. UK Parliament. Retrieved 3 April 2023. https://www.youtube.com/watch?v=p4_ogQcSJUU

UK Parliament 2020f. Covid-19: Contact-tracing App. Volume 803: debated on Wednesday 6 May 2020. UK Parliament Hansard in House of Lords. Retrieved 5 April 2023. https://hansard.parliament.uk/Lords/2020-05-06/debates/12B7E8EE-BD29-4E57-B5AC-7D014388B083/Covid-19Contact-TracingApp

UK Parliament 2020g. Covid-19: NHS Contact Tracing App Volume 803: debated on Monday 18 May 2020. UK Parliament Hansard in House of Lords. Retrieved 5 April 2023. https://hansard.parliament.uk/Lords/2020-05-18/debates/1AEBA78C-1807-46CB-BDC9-73937A380A9A/Covid-19NHSContactTracingApp

Appendix B. Examples of statements and how they are coded.

Text extract	Code
Germany	
The entire system is based on a voluntary principle. No one has to use this app. But millions of citizens should participate in order to reliably stop chains of infection and thus better protect each other.	Moral (with pragmatic)
The project is an example of what fighting this pandemic is about, beyond the health aspects: social cohesion and legitimacy, acceptance and trust - in democracy, but also in the constructive power of digital progress. The openly visible code of the app and thus its quasi-democratic audit are an opportunity to give this country a boost in digitization through broad consensus - not to the benefit of individual actors, for example in politics, in health care or the IT industry. But for the benefit of our entire society, to which every single person can make their contribution. Let's not let this chance slip by. Join us.	Moral
Telekom are doing everything we can to complete this app as quickly as possible. Fast, secure in accordance with #gdprcompliance (DSGVO) and fully transparent through #opensource: this is what we're striving for.	Pragmatic (with moral)
We have consciously chosen an open source approach because it creates trust. We need broad acceptance of the app among citizens, right from the start.	Moral
Data Privacy document: Details are outlined in the privacy notice of the Robert Koch Institute. Additional insights are available in the Data Protection Impact Assessment (German only), the Legal Notice for iOS and Android (German only, find English version in app) and the corresponding annexes 1a, 1b, 1c, 2, 3, 4, 5, 6, 7 and 8. Past versions of the respective privacy notice and the initial Data Protection Impact assessment are still available.	Pragmatic
Lothar Wieler of the Robert Koch Institute (RKI), Germany's leading public health advisory body, said the app would be an "effective tool to help us break chains of infection".	Pragmatic
This approach was chosen for the Corona-Warn-App in order to create trust through technological transparency and thus also to strengthen the acceptance of the app among the population. In addition, the disclosure and verifiability of the source code gives everyone the opportunity to actively contribute to the success of the solution, e.g. in the form of suggestions for corrections or improvements.	Moral
"I don't know anything about you, but I'll protect you." (Slogan at the government's press conference when the app was launched).	Moral

But to be clear: this app is not a panacea.	Non-cognitive
"People want it, it works, and it is helping prevent infections" (Jens Spahn)	Pragmatic
The pandemic has shown that every actor is important in the crisis: every person, every company, every institution is responsible for the big picture.	Moral
Two of the main priorities right now are the interoperability with coronavirus apps of other countries – especially in the European Union – and the availability of the German app in foreign app stores. The Robert Koch Institute recently shared that the Corona-Warn-App can now also be downloaded from app stores in all EU member states as well as Norway, Switzerland, and the United Kingdom.	Pragmatic
The architecture follows a decentralized approach – based on the DP-3T and TCN protocols, as well as the Privacy-Preserving Contact Tracing specifications by Apple and Google.	Pragmatic
Norway	
We are encouraging as many people as possible to download the app. Data on how we move and how many people we meet will be important to see how the infection prevention measures work, and how many more close contacts we have. As data is collected, you will receive a notification if you have been in close contact with an infected person and receive advice on how to deal with it.	Pragmatic
If many people download "Smittestopp", we can together shorten the period of intrusive measures, so that we can regain our freedom quickly.	Cognitive (with moral)
More updates will be made to the app in the future, among other things to improve universal design to ensure equal access for everyone.	Moral
The pandemic is not over. We have no immunity in the population, no vaccine, and no effective treatment. Without the Smittestopp app, we will be less equipped to prevent outbreaks that may occur locally or nationally.	Pragmatic
If we are to get our everyday life back, as many people as possible should download the app.	Cognitive
In order for us to be able to open up more in the coming weeks and months, there are several prerequisites that must be met. More automated and efficient tracking is one of these prerequisites. That is why I [Prime Minister] am asking you all to take part in another "Dugnad", to also work on tracing the infection, which we must do together, among other things, by using the Smittestopp app.	Cognitive (with moral)
Smittestopp is an app that is connected to several other things we want to do, such as testing more people, having a low threshold for when people can	Pragmatic

be tested and testing out in the population to know how widespread the infection is and how it will develop, and in addition, provide better for those isolating, and follow and study the development and impact of the measures. It is absolutely crucial to be able to stop measures that harm society and that are difficult to live with over time.	
I [PM] just want to say that we all want to return to a more normal everyday life. The everyday life where more people can go back to work, where the wheels of our economy start rolling again. Where society functions more like it did before the crisis started. Together, we have managed to beat down the virus and gain control over its spreading, but if we are to succeed in taking back more of our everyday life and at the same time control the infection, then we must take our own steps, which includes using this app. If we fail when we open, and cannot maintain control, then we have to tighten again. But to ensure that we have the right measures, this app will contribute towards that. And I think that is of great value, both for the individual and for society as a whole. Therefore, my appeal is that as many people as possible download this app and take part in a new dugnad.	Cognitive (with moral)
The app opens up something we have wanted for a long time. Namely that we can obtain information about movement patterns and contact patterns among app users. We can use that information to gain better knowledge about the spread of infection in society and better knowledge to predict the further development of the epidemic. Perhaps we will have to live with this epidemic for a long time and then it will be crucial throughout the period.	Pragmatic
Security has the highest priority in development. Simula has used well-established industry and encryption standards to secure the app, we have ongoing discussions with the Norwegian Data Protection Authority throughout the development period, and we have external suppliers specialized in security who look through the code and the solution.	Moral
Use of the app is voluntary. All personal data will be deleted after 30 days. You can delete your personal data at any time by using the delete functionality in the app, you can also delete the app itself.	Moral
Utility of the app: The app will have immediate utility in assessing what kind of measures work well and less well. For the individual, the utility value will come gradually when the app has been tried out, and eventually when notification via SMS can start in the event of close contact with infected persons.	Pragmatic
Downloading the Smittestopp app is voluntary. But it is not voluntary to participate in infection tracking.	Moral (with pragmatic)

It has been important for us to make the app as secure as possible. We have consulted with the Norwegian Data Protection Authority in the process, and the ministry has received help from IKT Norge to set up an independent expert group which was tasked with evaluating the app with a critical eye.	Moral
United Kingdom	
Today's launch marks an important step forward in our fight against this invisible killer and I urge everyone who can to download and use the app to protect themselves and their loved ones.	Pragmatic
We have prioritised security and privacy in all stages of the app's development, starting with the initial design, and user testing. We have drawn on expertise from across government and industry to review our design and help test the app. We are working with Apple and Google on their welcome support for tracing apps around the world. As part of our commitment to transparency, we will be publishing the key security and privacy designs alongside the source code so privacy experts can "look under the bonnet" and help us ensure the security is absolutely world class.	Moral
We are confident that every person who downloads the app will be helping to protect themselves and their loved ones.	Pragmatic
As much as the app has already had great adoption, downloads and reviews, new technology is always being developed – and we are continuing to upgrade the app to make it even better with the latest version released today, including a world leading approach to estimating distance which improves the accuracy of self-isolation notifications.	Pragmatic
We will always make sure the app is compliant with data protection law and meets the standards expected for data security and confidentiality.	Moral and pragmatic
Any use of data and information generated or collected by the app will comply with Data Protection law and the Common Law Duty of Confidentiality (where applicable).	Pragmatic
It is always your choice to use the app. If you do, it will share a limited amount of anonymised data with UKHSA.	Pragmatic
This new app has the potential to contribute towards the country returning to normality - but only if a large proportion of the population installs it. Which means that millions of us are going to need to trust the app and follow the advice it provides. To earn that trust,	Cognitive (with moral)

we will continue to work based on transparent standards of privacy, security and ethics.	
The app will give the public a simple way to make a difference and to help keep themselves and their families safe.	Pragmatic
Our absolute priority in this pandemic is to protect the NHS and save lives. We are working at pace to develop our test and trace service, which will significantly improve our ability to track the virus and stop the spread.	Pragmatic
The download numbers, the community engagement on the open source platform GitHub, and the feedback we received from independent experts confirm that this was the right approach. This transparency was key to increasing trust in and acceptance of the app in broad parts of society.	Moral
One of the things it has taught us is that it is the human contact that is most valued by people. There is a danger in being too technological and relying too much on texts and emails and alienating or freaking out people because you are telling them quite alarming news through quite casual communication.	Non-cognitive
Gran doesn't need the app to benefit from it. If you download the app, you're protected and you're more likely to be protecting the people you care about around you.	Pragmatic

Article 4: Attitudes towards government surveillance and the role of trust in a pandemic: A survey experiment in 16 European countries

Publication status: Under review in *Government Information Quarterly*.