Privacy, Informational Infrastructures and Covid-19: Comparative Legal Responses

Michael Veale, *Associate Professor, Faculty of Laws, University College London*

To appear in: Jeff King and Octavio Ferraz (eds.) Comparing Covid Laws: A Critical Global Survey (OUP 2024)

This version: 22 November 2023.

Abstract Covid-19 saw states creating and repurposing informational infrastructures to manage populations and in turn, the pandemic. In this chapter, I consider how these infrastructures played out in their legal contexts. I show how while privacy regimes, where they existed, largely remained applicable, particular technologies reshaped the privacy landscape and at times, pushed at the boundaries of the legal system. States seeking to use telecommunications data to shape behaviour faced significant legal challenges as courts struck down a range of instruments, although some powers proved nebulous and hard to challenge. Digital contact tracing apps showcased a different dynamic, as the architecture of these systems — whether centralised or decentralised — shaped legal responses. Not all is gloomy however — insofar as the pandemic made information technology a political focus for legislators and citizens, this may bode well for future law-making and governance.

I. Background

The most internationally widespread public health interventions recommended to reduce transmission of Covid-19 are relatively blunt tools, such as lockdowns or related restrictions. These brought deep consequences, including to social relations, economic activity and other aspects of public health. They triggered debates concerning proportionality and liberties and at times led to heated societal tension.

In both the anticipation and aftermath of these measures, there was immense interest in how blunt tools could be replaced over time with infrastructures that allowed more precise intervention. Contact tracing is a more precise technique than a lockdown, but in its classic,

manual form it is expensive, laborious and in many countries where it was deployed, it struggled to keep up with the scale and speed of transmission. Faced with this perceived challenge, widespread international demand emerged in 2020 for two main types of technologies:

Technologies for information gathering. The first category were technologies that provided access to faster or deeper information on the pandemic. Some of this information gathering can be seen as a more accelerated and pervasive form of the collection of information for research to reduce uncertainties about diagnosis and treatment, as well as to inform policy development. Such data collection poses interesting ethical and legal issues. For example, the more rapid collection of data through 'challenge studies' where individuals are heavily compensated to take heightened risks from unknown treatments,[1] enhanced linkage and analysis of medical record data which can open avenues for analysis that may break public expectations,[2] or controversies around the geopolitics of moving medical data around the world.[3] Some sources of information may be initially surprising in their nature — such as the use of wastewater and sewage analysis to detect variants[4] — but also have surprising analytic potential.[5]

The focus of this paper is not on information gathering for research, as important as that is, but on *operational data use*. While research data in the pandemic was filtered through scientific advisory mechanisms,[6] operational use of information creates a direct link with the action of the state and coercive powers granted to public health actors. Such information may support or even make frontline decisions, in ways with more or less automation present at different stages of the decision-making process.[7] In many situations, issues of privacy have been significantly implicated, particularly because data used were not gathered from typical healthcare actors or contexts, but often come from contexts where their use by public health actors or governments in general may not have been anticipated.[8] This does not mean that public health authorities lack potential authority to do this, but such data use —in many cases entirely novel — has created new linkages between telecoms, CCTV, location data, online tracking data, amongst other types. As we shall see, such highly sensitive data categories have often only been authorised for use by the national security apparatus, often (although not always) under specific and bespoke safeguards. Creating flows to other parts of the state without such safeguards can risk uses beyond those envisaged for public health, beyond these safeguards, due to a lack of pre-existing bespoke regimes for data acquisition and management.

---

[1] Euzebiusz Jamrozik and others, 'Key Criteria for the Ethical Acceptability of COVID-19 Human Challenge Studies: Report of a WHO Working Group' (2021) 39 Vaccine 633.

[2] Elizabeth J Williamson and others, 'OpenSAFELY: Factors Associated with COVID-19 Death in 17 Million Patients' (2020) 584 Nature 430.

[3] For example, such a situation emerged in the Indian state of Kerala during the pandemic, which became embroiled in a legal and political controversy around the US firm *Sprinklr*. See Jacob Jeemon, 'Kerala Backs out of Sprinklr Deal, Cancels Controversial Pact over Privacy Issues' (*India Today*, 21 May 2020) <https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21> accessed 11 June 2023.

[4] Lin Li and others, 'Detecting SARS-CoV-2 Variants in Wastewater and Their Correlation with Circulating Variants in the Communities' (2022) 12 Sci Rep 1, 16141.

[5] Reuben Binns, 'Data is the New Sewage' (Gikii 2020, 30 July 2020); see further a Twitter thread on more recently tracing an individual suspecte to be the source of a new variant in Ohio, US, Marc Johnson [@SolidEvidence], 'Ohio Cryptic Lineage Update. We've Made No Progress Identifying the Individual, but We Have Learned a Few Things. 1/ Https://T.Co/IE2GB6CwPO' (Tweet, 4 June 2023) <https://twitter.com/SolidEvidence/status/1665444603829407746> accessed 11 June 2023.

[6] See eg Kira Matus and others, 'From SARS to COVID-19: The Role of Experience and Experts in Hong Kong's Initial Policy Response to an Emerging Pandemic' (2023) 10 Humanit Soc Sci Commun 1, 1.

[7] Reuben Binns and Michael Veale, 'Is that Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR' (2021) 11 International Data Privacy Law 319.

[8] On the centrality of context within informational privacy, see Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

Technologies for population management. The second category of technologies were designed to reduce the need for blanket restrictions by targeting interventions through the profiling of individuals or communities. This is distinct from information gathering in the same way that Bentham's proposed Panopticon did not run a data processing operation, yet sought to enforce certain policies through architectural features. These technologies were not (necessarily) about the collection, perusal and application of data associated with visual metaphors of *surveillance*, but the creation of grammars of capture, orchestrating citizens to gather, act, and travel in certain ways and in adherence to certain policies.[9] Typical variants of two of the main technologies in this area, mobile contact tracing applications and vaccination certification, did not functionally rely on a public health actor 'gathering information' (although some variants have information gathering as an additional function). We can understand their core functionality as the enforcement of policies through infrastructure, often mobile devices, shaping conditions such as those under which an individual is asked to self-isolate, or under which they are permitted to enter a hospitality venue.[10]

These policies are intended to manage populations in a granular manner. Digital contact tracing systems, like their 'manual' counterparts, are designed to sort individuals into those that should stay in one place or receive a test versus those that need not to, focussing on managing individuals at the boundary of their house and the outside world based on their activities within it. Other technologies manage this boundary more directly, such as so-called 'digital fences',[11] which used apps,[12] cell tower data,[13] or wearables to enforce quarantine;[14] and systems for issuing digital authorisation forms for visits to shops, exercise or similar.[15] Certificates of vaccination, testing or recovery usually intend to manage populations on boundaries further away from the home, between non-essential spaces, such as bars or restaurants, and the world outside them. Some states additionally utilised drones with the aim of shaping the nature of outdoor interactions.[16] Designers of these infrastructures intend to alter the riskiness of activities, such as meeting in enclosed spaces or travel to areas vulnerable to some or all disease variants, by influencing the composition of individuals undertaking these activities rather than the nature or availability of the activities themselves.

Both of these technologies entail privacy interests of differing types. In part, this might be because of the breadth of interests captured by the term 'privacy' and the number of distinct conceptual levels in play (and often conflated) when that term is deployed.[17] Some conceptions of privacy focus on protecting information from being observed by others, linking it closely to confidentiality — a conception favoured by engineers due to its

[9] Philip E Agre, 'Surveillance and Capture: Two Models of Privacy' (1994) 10 The Information Society 101.
[10] Michael Veale, 'Verification Theatre at Borders and in Pockets' in Colleen M Flood and others (eds), *Pandemics, Public Health, and the Regulation of Borders: Lessons from COVID-19* (Routledge 2024); Stefania Milan and others, 'Promises Made to Be Broken: Performance and Performativity in Digital Vaccine and Immunity Certification' (2021) 12 European Journal of Risk Regulation 382.
[11] See generally Yoshiyasu Takefuji, 'Analysis of Digital Fences against COVID-19' (2021) 11 Health Technol 1383.
[12] See e.g. the UAE, George Sadek, 'United Arab Emirates' in Jenny Gesley and others (eds), *Regulating electronic means to fight the spread of COVID-19* (Law Library of Congress, Global Research Directorate 2020). See also Poland, Magdalena Brewczyńska, 'Poland: Policing Quarantine Via App' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).
[13] See e.g. Taiwan, Sung-Yueh Perng, 'Materialities of Digital Disease Control in Taiwan during COVID-19' (2022) 9 Big Data & Society 20539517221097315.
[14] See e.g. South Korea, Sayuri Umeda, 'South Korea' in Jenny Gesley and others (eds), *Regulating electronic means to fight the spread of COVID-19* (Law Library of Congress, Global Research Directorate 2020).
[15] See e.g. Greece, Evangelia (Lilian) Tsourdi and Niovi Vavoula, 'Killing Me Softly? Scrutinising the Role of Soft Law in Greece's Response to COVID-19' (2021) 12 European Journal of Risk Regulation 59.
[16] See e.g. Singapore, Croatia; Bojana Kostić and others, 'Western Balkans: Instruments of Chilling Politics' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020); Julienne Chen and Poorthuis Ate, 'Singapore: A Whole-of-Government Approach to the Pandemic' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).
[17] Kieron O'Hara, *The Seven Veils of Privacy: How Our Debates about Privacy Conceal Its Nature* (Manchester University Press 2023).

computational tractability.[18] Broader conceptions however focus on privacy's relationship with autonomy. This conception of privacy sees the value of the former mainly arises from helping secure aspects of the latter, providing the space for individuals to develop the capacities for self-determination and the management of the boundaries between themselves and their contexts.[19] Interference with these capacities does not necessarily require information to be 'gathered' about an individual, just as surveillance in a clothing shop might consist of a tag that is entirely passive until it triggers a loud beep to attract attention to discipline shoplifters from attempting a stealthy exit.

A. Legal background

There are significant differences in existing data and privacy law across states. Constitutional recognition of a right to privacy or private life varies internationally, and in many cases is still emerging through case law.[20] The right to privacy has long been recognised as an international human right,[21] but the right to protection of personal data is a more recent development emerging as related but distinct from the right to privacy or to private life.[22] In 2023, 137 out of 194 UNCTAD member states (United Nations Conference on Trade and Development) had some form of regime protecting data or privacy, including 98% of countries in the Europe region, 74% in the Americas, and 61% in Africa.[23] Just over a third of countries with no current regime have a draft law.[24] This has grown significantly in the 2010s, with 62 countries enacting new laws — more than in any previous decade.[25]

The protection of certain medical information is older and more widespread, whether through law or professional norms. Privacy is found in international medical ethics declarations, such as the Helsinki Declaration, which commonly make their way into national laws, guidelines or the regulatory documents of professional bodies.[26] Obligations of medical confidentiality are similarly recognised, but despite near-universal acceptance, are not always codified in law, particularly in the Global South.[27] Even where laws exist concerning confidentiality of medical information, their scope may be narrow, including only certain actors or information passed in the concept of clinical relationships, and thus exclude many times when the vast array of health-related information of interest in a pandemic is implicated.[28]

---

[18] See eg the discussion of privacy-as-confidentiality in Seda Gürses, 'Can You Engineer Privacy?' (2014) 57 Communications of the ACM 20.

[19] Beate Rössler, *The Value of Privacy* (Rupert Glasgow tr, Polity 2005); Julie E Cohen, 'What Privacy is For' (2012) 126 Harv L Rev 1904.

[20] See eg *Justice K.S. Puttaswamy v. Union of India* [2017] 10 SCC 1 (India).

[21] See eg Universal Declaration of Human Rights, art 12; International Covenant on Civil and Political Rights, art 17.

[22] See eg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 ('Convention 108'), ratified by over 55 states including many non-members of the Council of Europe including Argentina, Mexico, Morocco, Senegal and Uruguay; EU Charter of Fundamental Rights, art 8.

[23] United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide' (*unctad.org*, November 2023) <https://perma.cc/7LYM-6Z2X> accessed 18 November 2023.

[24] ibid.

[25] Graham Greenleaf and Bertil Cottier, '2020 Ends a Decade of 62 New Data Privacy Laws' (2020) 163 Privacy Laws & Business International Report 24.

[26] 'Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects' (Adopted by the 18th World Medical Assembly, Helsinki, Finland, June 1964 and as revised by the 29th World Medical Assembly, Tokyo, Japan, October 1975 1975) para 6.

[27] Privacy International, 'Medical Privacy and Security in Developing Countries and Emergency Situations' (March 2012) 10 <https://perma.cc/3388-JQSC> accessed 5 November 2021.

[28] See e.g. in a United States context, Latena Hazard, 'Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities' (2017) 25 Catholic University Journal of Law and Technology 447; Lawrence O Gostin and others, 'Health Data and Privacy in the Digital Era' (2018) 320 JAMA 233 (on how HIPAA 'creates artificial distinctions between data generated in clinical or health insurance settings and in online settings').

B. Structure of this chapter

As both the regulation of information gathering and population management relate to broader and often horizontal privacy regimes, I will first highlight the ways (and extent to which) privacy regimes in general were amended or set aside during the pandemic. I then turn to two issues of the specific interaction of law and information technology — the use of telecoms data for surveillance, and the development and regulation of varied forms of digital, mobile contact tracing. These are just a handful of informational infrastructures we could consider — the creation and use of electronic health records where they may have been absent or little-used before; the handling of 'manual' contact tracing data; the deployment of vaccination and test certification. However, I have chosen the above due to their shared focus on population management — these were technologies designed to make populations legible, and shape their actions and activities at a granular level that is simply not possible without information processing.

More broadly, we can see pandemics as sites of 'liminal surveillance', where heightened expansion, testing and experimentation with surveillance systems and their associated legal regimes may be legitimate or accepted for a period of time. This may allow the actors involved to either directly normalise it in the period following, or gather the resources and evidence to normalise these heightened practices.[29] Liminal surveillance is often studied during large events, such as international sporting competitions,[30] but the Covid-19 pandemic can be understood as such a site as well.[31] The below examples illustrate such liminal surveillance in legal context — and may as such shed light on how different institutions and actors react when faced with large and significant new infrastructures in a crisis.

II. Privacy regimes in a pandemic

Some — but perhaps surprisingly few — states sought to suspend the effect or enforcement of horizontal data protection rules during the pandemic. In **Hungary**, all data controllers were allowed to refuse access, objection, erasure, portability or procedural automated decision rights to data subjects during the period of the state of emergency, which attracted criticism from European regulators.[32] While the General Data Protection Regulation, an EU regulation with direct effect upon EU members, permits Member States to restrict certain of its rights, this is only possible if such restrictions '[respect] the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard'.[33] While this provision was challenged in court, initially challenge was not decided on the merits, instead dismissed based on the decree no longer being in force and no cases where the

[29] Kees Boersma, 'Liminal Surveillance. Intensified Use of an Existing CCTV System during a Local Event' (2013) 11 Surveillance & Society 106.

[30] See eg the French alteration of domestic law to allow AI-powered surveillance cameras during the 2024 Olympics in *Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, dernière modification le 25 juillet 2023* (France); see also its confirmation as legal within the French regime by the *Conseil constitutionnel* in *Décision n° 2023-850 DC du 17 mai 2023* (France).

[31] Eula Bianca Villar and John Pascual Magnawa, 'Surveillance and Pandemic Governance in Least-Ideal Contexts: The Philippine Case' (2022) 30 Journal of Contingencies and Crisis Management 22.

[32] European Data Protection Board, 'Thirtieth Plenary Session: EDPB Response to NGOs on Hungarian Decrees and Statement on Article 23 GDPR' (*EDPB*, 3 June 2020) <https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en> accessed 9 August 2023.

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (GDPR) art 23.

relevant rules were applicable; later a requirement for state agencies to explain their reliance on these restrictions was introduced.[34]

More common was explicit or implicit enforcement discretion. In the **United States**, from April 2020, the federal Department of Health and Human Services published a series of noticed of enforcement discretion relating to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, designed to support the use of information for public health.[35] The impact of this changes was limited however due to the intrinsically narrow scope of entities that are covered by HIPAA, which does not define its material scope by the nature of the data in question, and therefore omitted many important actors such as application developers or telecoms firms that may have been processing data for purposes relating to Covid-19.[36]

In the **United Kingdom**, some high-profile ongoing data protection investigations were suspended,[37] with the regulator emphasising that in light of the way in which a 'reduction in organisations' resources could impact their ability to comply with aspects of the law', the regulator would '[take] into account the impact of the potential economic or resource burden [its] actions could place on organisations'.[38]

In general, the Covid-19 pandemic saw a rapid digitisation across sectors — and such digitisation raised inevitable privacy concerns. Regulators faced a balancing act between not hindering the rapid adoption of technologies needed to continue crucial societal activities, such as education, and ensuring that this rapid adoption did not undermine data protection or privacy law. This is particularly important as software and hardware decisions create path dependencies, where it becomes expensive and organisationally difficult to shift providers after initial technical foundations are laid, and those technical foundations facilitate and foreclose certain future directions. It is perhaps telling that the EDPB report on public sector enforcement, which lists national European data protection authority action against public sector in relation to 'cloud' services in reverse chronological order, has a large gap between April 2020 and October 2020, where no enforcement action of this type was reported, despite the rapid digitisation.[39] Other topics saw divisions between data protection authorities. For example, on the issue of whether medical data such as temperature could be mandated from employees, some data protection authorities (at least **France**, **Italy**, **Hungary**, **Lithuania**, **Belgium**, **Luxembourg** and the **Netherlands)** discouraged this practice in guidelines while some considered it up the employer (**Greece**, **Switzerland**, **Ireland**, **Iceland**, **Spain**, **Russia** and **Slovakia**).[40] In part this may reflect a difference in regimes, but within in the EU at least, while it is theoretically possible for Member States to diverge and create employment-

[34] Fruzsina Gárdos-Orosz and others, 'Hungary: Legal Response to Covid-19' in Jeff King, Octavio Ferraz and others (eds), *Oxford Compendium of National Legal Responses to Covid-19* (OUP 2022) paras 55–56.
[35] Lindsay F Wiley and others, 'United States: Legal Response to Covid-19' in in Jeff King, Octavio Ferraz and others (eds), *Oxford Compendium of National Legal Responses to Covid-19* (OUP 2022) para 190.
[36] Stacey Tovino, 'At a COVID Crossroads: Public Health, Patient Privacy, and Health Information Confidentiality' (2021) 65 Saint Louis University Law Journal, 857.
[37] Information Commissioner's Office, 'ICO Statement on Adtech Work' (*ICO*, 7 May 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/> accessed 5 November 2021.
[38] Information Commissioner's Office, 'The ICO's Regulatory Approach during the Coronavirus Public Health Emergency' (*ICO [only available via the Internet Archive]*, 15 April 2020) <https://web.archive.org/web/20200417022620/https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf> accessed 5 November 2021.
[39] European Data Protection Board, '2022 Coordinated Enforcement Action: Use of Cloud-Based Services by the Public Sector' (*EDPB*, 17 January 2023) <https://perma.cc/TR78-6UTX> accessed 19 November 2023.
[40] Evelina Pappa, 'Κορωνοϊός, θερμομέτρηση και προστασία προσωπικών δεδομένων (Coronavirus, temperature measurement and personal data protection)' (*Lawspot*, 1 May 2020) <https://www.lawspot.gr/node/267614> accessed 20 November 2023.

specific rules around data protection, few have actually done so with any substance or specificity, and so the law on the books remains in principle largely the same.[41]

Not all regulators showed deference to governments or other actors involved in pandemic response. In relation to bone fide public health data sharing and usage, data protection law gives a wide leeway to states during times of crisis. In EU data protection law, which has informed relevant statutes in many jurisdictions, monitoring epidemics is explicitly listed as a type of data processing that justifies the processing of both normal and sensitive categories of personal data.[42] Safeguards and care to respect rights and other processing principles are still necessary, and data still has to be *necessary* for this purpose, but reports of a fundamental clash between privacy and public health are often overstated. Despite this, in Italy, the data protection authority fined the INPS twice; firstly for a data breach which revealed other users' data in a form when individuals were trying to claim Covid-19 related financial support, and secondly related to the illegal use of data in attempted fraud detection when calculating Covid-19 bonus eligibility.[43] Norway also notably suspended a digital COVID-19 app and ordered bulk data deletion (discussed below).

III. Expansion of open-ended telecommunications data collection and access

Some states took the opportunity to utilise the pandemic to attempt to install more invasive general surveillance regimes and infrastructures, particularly in relation to telecommunications.[44] Telecoms data is important in a global context for both information gathering and population management as mobile phones (smart or not) are without doubt the most commonly owned sensing device held by individuals. While smartphone penetration as well as mobile Internet connectivity varies intensely across demographics and geographies, basic mobile connectivity and ownership is widespread. This in turn has rendered populations in the Global South rapidly more legible to governments, firms, international organisations and researchers, who have sought to track and understand human mobility through datasets based on signals triangulated between mobile phone masts.[45] Many jurisdictions sought aggregated mobile phone data to understand broad mobility patterns for telecoms operators, which should not, if done correctly, reveal anything about individuals.[46] This practice — while it may have some legal issues — is not the focus here.[47] Instead, I consider the expansion of individualised data sharing from telecoms companies, and the changes in the legal regimes governing this sharing.

---

[41] Halefom H Abraha, 'Hauptpersonalrat Der Lehrerinnen: Article 88 GDPR and the Interplay between EU and Member State Employee Data Protection Rules' [2023] The Modern Law Review.

[42] GDPR, recital 48.

[43] Garante per la Protezione dei Dati Personali, 'Provvedimento del 25 febbraio 2021 [9556958]' (25 February 2021) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9556958> accessed 8 November 2021; Garante per la Protezione dei Dati Personali, 'Provvedimento sui data breach INPS: comunicazione agli interessati coinvolti - 14 maggio 2020 [9344061]' (14 May 2020) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9344061> accessed 8 November 2021.

[44] Establishment of Emergency Communications System Instrument 2020 (Ghana).

[45] Linnet Taylor, 'No Place to Hide? The Ethics and Analytics of Tracking Mobility Using Mobile Phone Data' (2016) 34 Environ Plan D 319.

[46] See e.g. Kristofer Ågren and others, 'The Use of Anonymized and Aggregated Telecom Mobility Data by a Public Health Agency during the COVID-19 Pandemic: Learnings from Both the Operator and Agency Perspective' (2021) 3 Data & Policy e17; Pedro Rente Lourenco and others, 'Data Sharing and Collaborations with Telco Data during the COVID-19 Pandemic: A Vodafone Case Study' (2021) 3 Data & Policy e33.

[47] For those interested in probing the legal issues, one might ask what the legal basis under e-Privacy law was for accessing such communications data in order to later aggregate it.

A. Subscriber data

Subscriber data relates to information about the individuals in a communications system, rather than the contents of the communication itself.

Some states took steps towards increasing legibility of their populations through establishing infrastructures more capable of readily identifying individuals in the future — effectively increasing the amount of data kept on subscribers. In **Ghana**, an Executive Instrument (EI 63) was signed in March 2020 to create a national database linking individuals to phone numbers to phone models (IMEI numbers). Commentators described this as '[exploiting] a public health crisis to legislate for all public emergencies',[48] and emphasised that less intrusive legal means to request data around specific users, rather than a pre-emptive dataset of all users were already possible in Ghanaian law.[49] This instrument and its legal basis was later successfully challenged in the Accra High Court in 2021.[50]

Some states sought to increase the sharing of existing subscriber data with more state entities. In **Brazil**, the Federal Government passed an executive order in April which mandated telecommunications firms to share data including the name, telephone number and address of all consumers, in order to support pandemic-related statistical research.[51] The order included 'minimal guarantees' in relation to the requested data. In May, the Supreme Court, following a series of injunctions and judicial opinions, voted that the order was unconstitutional, finding that it was outside the scope of the emergency powers it was adopted under, and that, it did not respect necessity, purpose, adequacy, and information security.[52] This ruling marked a turning point for recognising that the constitution of Brazil requires data protection for data that is not secret or confidential, and accelerated the implementation of the Brazilian data protection legislation.[53]

B. Communications data

Communications data typically refers to information about communications of entities, but not including the content of these data. While subscriber data is more static metadata about the entities communicating, communications data is metadata relating to the network of communications, including where individuals were when they occurred.[54] In some states,

---

[48] Smith Oduro-Marfo, 'Ghana: Transient Crisis, Permanent Registries' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020) 142.

[49] MFWA, 'Ghana: MFWA Welcomes High Court Ruling Ordering Government to Stop Collecting Personal Data' (*Media Foundation For West Africa*, 2 August 2021) <https://www.mfwa.org/ghana-mfwas-welcome-high-court-ruling-ordering-government-to-stop-collecting-personal-data/> accessed 7 November 2021.

[50] *Rancis Kwarteng Arthur v Ghana Telecommunications Company Limited & 4 Ors*, Suit Nos. HR 0064/2020 and GJ 0855/2020 (High Court, Accra, Judgement of 22 July 2021) (Ghana). See generally Delali A Gawu and Richard Obeng Mensah, 'COVID-19 Contact Tracing and Privacy Rights in Ghana: A Critical Analysis of the Establishment of Emergency Communications System Instrument, 2020 (EI 63)' (2021) 65 Journal of African Law 361.

[51] Medida Provisória No. 954/2020 (Brazil).

[52] Direct Action of Unconstitutionality 6387, 6388, 6390 and 6393, *Federal Council of the Brazilian Bar Association, Brazilian Social Democracy Party, Brazilian Socialist Party, Socialism and Liberty Party, Communist Party of Brazil v Federal Government* – Provisional Measure n. 954/2020, DJe. May 7th, 2020 (Brazil).

[53] Nathalie Fragoso and others, 'Surveillance and Pandemic in Brazil: An Essay in Three Acts' in *Pandemic Surveillance* (Edward Elgar 2022); Bruno Ricardo Bioni and others, 'A Landmark Ruling from the Brazilian Supreme Court: Data Protection as an Autonomous Fundamental Right and Informational Due Process Case Notes' (2020) 6 Eur Data Prot L Rev 615.

[54] These definitions can be slippery in the context of intelligence and surveillance law, as some regimes try to transform content into communications data to benefit from the lessened protections afforded to metadata — for example, noting that these communications contain certain characteristics, which may have been gleaned by automated analysis. Graham Smith, *Internet Law and Regulation* (Sweet and Maxwell 2020) para 8.3.5; Graham Smith, 'The Content v Metadata Contest at the Heart of the Investigatory Powers Bill' (*Cyberleagle*, 26 May 2016) <https://www.cyberleagle.com/2016/05/the-content-v-metadata-contest-at-heart.html> accessed 19 November 2023. In this paper I work with the plain English meaning of these terms rather than the largely unresolved obfuscation some regimes, notably that of the United Kingdom, tries to create.

Covid-19 provided a means to demonstrate that data on individuals' activities rather than just their identities or devices could be accessed with only an executive order.

In **Israel**, location metadata was available for epidemiological investigations, with the Israeli Security Agency utilising a tool to obtain and analyse data on the request of the Ministry of Health.[55] The relevant powers underwent several modifications over the course of the pandemic, including some narrowing of scope, and a demand for primary legislation by the Supreme Court.[56] Pressure from civil society, and also the national privacy agency, which was initially denied a formal role in oversight and later gained a more prominent voice, albeit one without teeth, did somewhat strengthen oversight over the Israeli Security Agency, somewhat 'piercing the veil of secrecy surrounding Israel's SIGINT oversight ecosystem', but this appears to have been an ephemeral change.[57]

In **Poland**, an executive order in the absence of a state of emergency allowed the Minister for Digital Affairs to access location data of infected and quarantined persons from telecommunications providers.[58] Several other EU states, such as **Croatia**, attempted or contemplated such a move, but put this on hold in the face of public criticism.[59] In **Slovakia**, the 'Lex Corona', containing similar powers, was fast-tracked through parliament in 24 hours, yet in May the parts of the law relating to telecoms data access were suspended by the Constitutional Court due to the potential abuse of the accessed data by the state and the lack of safeguards contained within the law itself, among other elements.[60] While Parliament introduced an amendment to the law, in particular requiring consent of the data subject, it still did not respond to the court and allow a supervisory authority to regulate this power's usage.[61] In **Bulgaria**, amendments to the Electronic Communications Act were made which would allow public health authorities to obtain location information from telecommunications providers if individuals did not perform mandatory isolation or treatment. A challenge on substantive grounds against these provisions was lodged in April 2020 in the Constitutional Court.[62] In November 2020, the Court found these provisions unconstitutional due to the obligation for general retention of data on all individuals for six months that these provisions required.[63] For such EU Member states, these actions are more controversial given that CJEU case-law indicates that such retention requirements on telecommunications providers and access to traffic and location data is only permissible 'purposes of safeguarding national security, combating serious crime and preventing serious threats to public security', with limited geographic and temporal scope, and subject to 'clear and precise rules' regarding the procedural and substantial conditions and safeguards associated with these interferences with individuals' rights.[64]

---

[55] Amir Cahane, 'Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Location Tracking as a Test Case' (2021) 19 The University of New Hampshire Law Review 451, 472; Amir Cahane, 'The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers' (*Lawfare*, 21 March 2020) <https://www.lawfaremedia.org/article/israeli-emergency-regulations-location-tracking-coronavirus-carriers> accessed 9 August 2023.

[56] Einat Albin and others, 'Israel: Legal Response to Covid-19' in Jeff King, Octavio Ferraz and others (eds) *Oxford Compendium of National Legal Responses to Covid-19* (OUP 2022) paras 157–158.

[57] Cahane (n 55).

[58] Brewczyńska (n 12).

[59] Daniel Kostić and others, 'Western Balkans: Instruments of Chilling Politics' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).

[60] PL. ÚS 13/2020-103 (Slovakia). See generally Matúš Mesarčík, 'Digital Surveillance in the Times of COVID-19: Lessons from Slovakia' (2020) 8 European Journal of Transformation Studies 184.

[61] ibid.

[62] Denitza Toptchiyska, 'Protection of Privacy in the Period of Covid-19 Pandemic' (2020) 16 Law Journal of New Bulgarian University 2, 63.

[63] Constitutional Court of Bulgaria, Decision No. 15 of November 17, 2020 in constitutional case No. 4 of 2020. https://www.constcourt.bg/bg/act-6866 (Bulgaria).

[64] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791, para 168.

In **Peru**, legal changes under emergency powers were made to permit the sharing of historic phone geolocation data with emergency health services when people appeared to have Covid-19.[65] The following year, individuals entering the country were also forced to consent to the sharing of geolocation data from their phones, with the unclear meaning or legal basis for this highlighted at the time by civil society.[66]

C. Orders with unknown scope

In other states, similar measures appeared to be taken but without obvious legal grounds. Similar declarations of data collection from telecommunications providers were made in **Uganda**, with information dispersed across ministries in such a way that information about this initiative, its scope and legal basis remain unclear.[67] In **Serbia**, it was announced that 'Italian phone numbers' were being tracked, raising suspicions of unaccountable and unlawful mass surveillance measures.[68] In **South Africa**, initial ministerial directions instructed mobile operators to provide telecommunications data such as location with no limitations on the purpose of data collection or who could access the data within the public sector.[69] These were later replaced by an amendment to the law which was more limited in nature, although the state of the previous directions remains unclear.[70] Such secretive, open-ended provisions made by ministerial direction are reminiscent of the general purpose orders that underpinned the early UK framework for data retention by telecommunications operators,[71] and which were found to be in violation of human rights obligations whilst their existence until their 'avowal' into the public domain.[72]

IV. Digital contact tracing systems and the law

Digital contact tracing systems are new infrastructure never explicitly anticipated in existing law. As such, they brought both implications for privacy and information, contestations over power and the control of different architectures, and were often accompanied by a range of legal frameworks. Unlike some pandemic-related digital systems such as 'digital fences' for quarantine enforcement, digital contact tracing systems were deployed in a very large number of jurisdictions, often installed on devices by a significant proportion of the adult population.

Several types of digital contact tracing systems exist. Here, I focus on two approaches. The first approach is *digital proximity tracing*, triggering interventions for individuals who had significant direct exposure, in terms of time and distance, to other individuals later suspected to be infectious at that time.[73] While many technologies could be used to indicate difference, issues such as reliability, ubiquity and battery consumption meant that these apps

[65] Dilmar Villena, 'Te Cuido Perú: Analizando la constitucionalidad de la geolocalización' (*Hiperderecho*, 18 April 2020) <https://hiperderecho.org/2020/04/geolocalizacion-constitucional-operadoras-peru-covid/> accessed 10 August 2023.
[66] Lucía León Pacheco, 'Esto es lo que sabemos sobre la autorización de geolocalización que solicita Migraciones para el ingreso al territorio peruano' (*Hiperderecho*, 23 March 2021) <https://hiperderecho.org/2021/03/esto-es-lo-que-sabemos-sobre-la-autorizacion-de-geolocalizacion-que-solicita-migraciones-para-el-ingreso-al-territorio-peruano/> accessed 10 August 2023.
[67] Daniel Mwesigwa, 'Uganda: Guerrilla Antics, Anti-Social Media and the War on the Pandemic' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).
[68] Kostić and others (n 59) 295.
[69] Alison Gillwald and others, 'South Africa: Protecting Mobile User Data in Contact Tracing' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).
[70] ibid; Petronell Kruger and others, 'South Africa: Legal Response to Covid-19' in in Jeff King, Octavio Ferraz and others (eds), *The Oxford Compendium of National Legal Responses to Covid-19* (OUP 2021) s VI.B.
[71] Telecommunications Act 1984, s 94 (United Kingdom, repealed).
[72] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2017] UKIPTrib IPT_15_110_CH (United Kingdom).
[73] See generally Carmela Troncoso and others, 'Deploying Decentralized, Privacy-Preserving Proximity Tracing' (2022) 65 Commun ACM 48.

predominantly were deployed on smartphones and utilised Bluetooth Low Energy signals, although the ways different systems used information passed using these signals varied in important ways. The second approach, which typically came later after some societal 'opening up', is *digital presence tracing*, where, particularly in response to the growing recognition of airborne transmission of Covid-19, interventions were triggered based on co-location of an individual with one or more individuals later suspected to be infectious at that time in largely indoor venues, even when these individuals may not have been within close proximity of each other.[74] These systems predominantly relied on individuals 'checking-in' to locations, typically involving venue-specific websites, or QR codes that could be scanned with a smartphone's camera.

A. Data processing in contact tracing systems

The type of data processed by these systems varied considerably depending on the systems' design and operation. The earliest proximity tracing proposals (for example, Singapore's *Bluetrace*) were *centralised*. In response to these, in March 2020, there was an emergence of *decentralised* proposals, firstly the DP-3T system[75] and the Apple-Google *Exposure Notification* system based on upon it. A significant debate emerged concerning the choice between these two architectures of system.[76]

The term 'decentralisation' related to the existence or absence of a centrally accessible social graph (a computational representation of a network) of who-saw-who. In centralised systems, such a graph either existed by design or could be retrieved or reconstructed due to the technical features of the system. Such a graph would inevitably reveal sensitive information about human relations and is intrinsically valuable data because it is hard to accurately come across. Online versions of graphs are commonly attributed to an overwhelming part of the value of firms such as Facebook or LinkedIn, the latter of which sold for $26bn to Microsoft in 2016, with the potential to map and understand economy and society,[77] but highly complete physical equivalents of such graphs do not exist, at least not in public and outside the intelligence community, were they to be inferred from telecoms data.

Decentralised proximity tracing systems broadly work by having a user's device capture and store locally information about the phones it was near, like a diary, and then regularly download a list of phone identifiers connected to people who since tested positive, and if a match of significant duration and proximity is found, to notify the user. A centralised system broadly worked by phones emitting encrypted contact details that could be decrypted by a government server, and other individuals' phones storing them when they are seen. When an individual tests positive, they upload all the individuals they have seen in that time period, and a central server decrypts the captured details, calculates which exposures are risky, and contacts the individuals implicated.

Presence tracing system are less studied and more heterogenous, but function similarly. Decentralised systems see individuals keep a diary of where and when they have been (e.g. by scanning QR codes in hospitality venues, and regularly downloading a list of exposed

[74] See e.g. Wouter Lueks and others, 'CrowdNotifier: Decentralized Privacy-Preserving Presence Tracing' (2021) 2021 Proceedings on Privacy Enhancing Technologies 350.
[75] Carmela Troncoso and others, 'Decentralized Privacy-Preserving Proximity Tracing' (2020) 43 IEEE Data Eng Bull 36. The author of this piece is one of the authors of this system.
[76] Tamar Sharon, 'Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers' (2021) 23 Ethics Inf Technol 45; Michael Veale, 'Sovereignty, Privacy and Contact Tracing Protocols' in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).
[77] Steve Atchison, '$26 Billion and the Incalculable Value of LinkedIn' (*Vox*, 15 June 2016) <https://www.vox.com/2016/6/15/11937240/microsoft-linkedin-deal-economic-graph-professional-data> accessed 20 November 2023.

locations and comparing them to the diary. Centralised systems varied, but would typically expose visitor information either to a central server, or to the venues themselves.

The purpose of this paper is not to reopen a substantive debate on the merits of different systems, but it is worth outlining the differences. Broadly, the debate between centralised and decentralised systems proximity tracing systems hinged on proponents of a decentralised approach noting the risks of centralising a social graph and the absence of a technical need for it to exist in order to make a system that notified individuals of their past proximity to those who later tested positive. They noted that ensuring adoption was more important than highly speculative benefits that might come from the collection of this graph, and that as it was effectively impossible to interoperate decentralised and centralised systems across borders, the choice of a centralised system, even in a more trusted jurisdiction with strong rule-of-law protection, would force many weaker regimes with poor human rights records into a centralised model that was open for abuse.

In contrast, the proponents of a centralised regime speculated that there were such potential operational and/or analytic benefits from the visibility of this graph that outweighed any negative impact a more revealing technology might have on adoption. Furthermore, after Apple and Google announced their Exposure Notification system, a small number of governments, typified by **France**, made arguments around digital sovereignty and determining their own system on principle. Presence tracing systems differed in similar ways but were less subject to a common international debate, instead being connected to particular incidents, outlined further below.

B. Mandatory or voluntary?

While proximity and presence tracing apps were often voluntary, this was not the case everywhere. In **India**, the centralised *Aarogya Setu* contact tracing app was first made mandatory for individuals in containment areas, with obligations placed on employers to ensure full adoption by their employees.[78] This was later diluted to a 'best effort' standard, although the *de facto* mandatory nature of the app in many spheres of society led to a series of legal challenges which clarified a voluntary status for it.[79] In **Qatar**, the Ehteraz app was made mandatory for all citizens and residents in Qatar from 22 May 2020 by a decision of the Council of Ministers.[80] While the government asserted that no other agencies could access data from the app, no legal instrument enacted this protection.[81] In the **UAE**, the Alhosn app was an omnibus system incorporating centralised Bluetooth contact tracing, quarantine control via linked wristbands, vaccine certification and a 'green pass' following testing. While the app was reported as voluntary, the UAE government announced that individuals who contract the virus and fail to download the app following this face a 10,000 AED fine, although law firm Norton Rose Fulbright note that it is 'unclear how this penalty has been implemented'.[82]

Some jurisdictions did not quite make apps fully mandatory, but did require it in certain contexts, or use incentives or other mechanisms to promote uptake. In **Singapore** in 2021 the government effectively mandated 'TraceTogether-only SafeEntry' in workplaces, mandating

[78] *Ministry of Home Affairs Order No 40-3/2020-DM* (1 May 2020) (India) <https://perma.cc/6JWT-AYC5>.
[79] See Aparna Chandra and others, 'India: Legal Response to Covid-19' in Jeff King, Octavio Ferraz and others (eds), *Oxford Compendium of National Legal Responses to Covid-19* (OUP 2023) s IV.A.9.
[80] Council of Ministers Decision of 18 May 2020 (Qatar). Published via the Qatari News Agency <https://perma.cc/29MX-4AFE>.
[81] 'Qatar Makes COVID-19 App Mandatory, Experts Question Efficiency' (*Al Jazeera*, 26 May 2020) <https://www.aljazeera.com/news/2020/5/26/qatar-makes-covid-19-app-mandatory-experts-question-efficiency> accessed 22 November 2023.
[82] Adjou Ait Ben Idir and others, 'Contact Tracing Apps in the United Arab Emirates' (*Norton Rose Fulbright*, 17 June 2020) <https://perma.cc/8HC7-XV4A> accessed 22 November 2023.

employers to facilitate contact tracing in a manner that effectively required employees to use these apps or Bluetooth 'tokens',[83] and providing 'BluePass tokens' to largely migrant construction workers for this purpose.[84] While at that stage these tokens did not appear to be legally mandatory, researchers with privileged access to such data described them as such, raising questions about how they were presented to such workers.[85] The government also mandated 'TraceTogether-only SafeEntry' for malls, effectively expanding the presence tracing system to also require the proximity tracing system to be used.[86] In **England and Wales**, the government attached a lightweight tracing system to the Bluetooth contact tracing system and made it a way to discharge the mandatory obligation to sign into venues without giving any details, making the proximity tracing app extremely popular and highly installed as a result.[87] In **Vietnam**, short-term visitors to the country were exempt from quarantine if they downloaded and used the BlueZone contact tracing app.[88]

In stark contrast to the above, **Australia** was an exceptional jurisdiction which created a new offence, with a maximum of 5 years imprisonment or 300 penalty units (then around 66,600 AUD) to take any adverse action or prohibit somebody access to premises on the grounds they were not using the national COVIDSafe proximity tracing app.[89]

C. Bespoke legal regimes or architectural protection?

States which adopted decentralised systems often argued that protection by the architecture of the system which limited data collection was a reason to tend not to enact further specific legal protection. For example, the **UK** and **New Zealand** explcitly resisted calls for legislation on the basis that their respective apps were decentralised.[90] Indeed, in the UK, an expert ethics group was set up when an early centralised app was in development, but after the centralised effort was abandoned in favour of a decentralised version based on Apple and Google's Exposure Notification, the ethics group was disbanded — as if no ethical issues existed any more.[91]

In contrast, the few states that adopted specific novel legal protections or limitations on app data access in relation to crime prevention, including **Australia** and **Singapore**, utilised a centralised contact tracing model. This is potentially because some of these regimes were reactive in nature. Both jurisdictions were embroiled in scandals when contact tracing data from centralised presence and proximity tracing systems was used for the purposes of criminal investigation. In Australia, a scandal of this type relating to a mandated QR check-in presence tracing app in Western Australia led to rapid passing of new legislation forbidding

[83] Workplace Safety and Health (COVID-19 Safe Workplace) Regulations 2021 (Singapore) s 22.
[84] Ministry of Manpower, 'Joint MOM-BCA-EDB Press Release on Enabling Targeted Quarantining through Contact-Tracing Devices for More than 450,000 Workers' (*Ministry of Manpower Singapore*, 16 October 2020) <https://www.mom.gov.sg/newsroom/press-releases/2020/1016-enabling-targeted-quarantining-through-contact-tracing-devices> accessed 22 November 2023.
[85] Yinxiaohe Sun and others, 'Use of Bluetooth Contact Tracing Technology to Model COVID-19 Quarantine Policies in High-Risk Closed Populations' (2023) 9 DIGITAL HEALTH 20552076231178418.
[86] 'TraceTogether-Only SafeEntry Brought Forward To 17 May 2021 To Enhance Coverage And Speed Of Contact Tracing' (Smart Nation Singapore, 4 May 2021) <https://www.smartnation.gov.sg/media-hub/press-releases/tos-17-may/> accessed 22 November 2023.
[87] The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020.
[88] Circular No 4674/BYT-MT on Guidance on Covid-19 Prevention and Control Regarding Short-Term Work Visits (Less than 14 Days) of Foreigners (Vietnam) <https://perma.cc/F5CT-99XC>.
[89] Privacy Amendment (Public Health Contact Information) Act 2020 (Australia) s 94H(2).
[90] Phil Pennington, 'Covid-19 App Data Protection: Government Resists Calls for New Law' (*RNZ*, 8 September 2021) <https://perma.cc/F6VB-HZLA> accessed 5 November 2021; HM Government, 'JCHR Report on COVID-19 Human Rights Implications: Government Response (CP 335)' (*GOV.UK*, 14 December 2020) 42 <https://www.gov.uk/government/publications/jchr-report-on-covid-19-human-rights-implications-government-response> accessed 5 November 2021.
[91] James Wilson and others, 'Providing Ethics Advice in a Pandemic, in Theory and in Practice: A Taxonomy of Ethics Advice' [2023] Bioethics.

the practice, after police did not agree to stop the practice until their powers were curbed.[92] At the Australian federal level, the national Bluetooth *proximity* tracing app was accompanied upon its introduction with strict secondary legislation, later replaced by primary legislation, which foreclosed this possibility.[93] In Singapore, the revelation that data access to the central repositories of information created by the Bluetooth proximity tracing app *TraceTogether* and the QR presence tracing app *SafeEntry* was occurring pursuant to the Criminal Procedure Code led to the passing of amendments which restricted this practice to serious offences only.[94]

An interesting exception and illustration of the interaction of architecture and law in the pandemic is **Belgium**. There, a decree specified the detailed technical specifications of a Bluetooth proximity tracing app in such a way that only a decentralised system could be legally designed and implemented, as well as specifying that, by design, it must 'not be possible' to use the system for other purposes.[95]

Where there was no specific legislation to address the limits of use of centralised systems explicitly, this could leave jurisdictions in quite uncertain territory. For example in **Germany**, requests to restaurants by the police for guestlist data collected for the purpose of infection control are in murkier waters, and whether this is explicitly forbidden may additionally differ by Länder, typically relying on pre-existing legal frameworks.[96]

D. Decentralised systems and limitations of enforcement

England and Wales[97] presented a further interesting example of the interaction of privacy, code and law in relation to the presence tracing system designed to scan QR codes ('NHS COVID-19'). The situation from September 2020 to March 2021 was that certain premises, such as restaurants, were obliged to request that all individuals aged 16 or over entering them either i) provide their contact details manually, or ii) scan the QR code which these venues were also obliged to print a copy of and display.[98] The QR code presence tracing system was decentralised in nature, meaning that upon scanning the QR code, it was not the case that details about the scanner were uploaded to a database, but instead details about the *venue* were saved to the phone, along with a timestamp. The phone would frequently download a list of locations flagged as risky, and would notify ('ping') individuals of what they should do. This created two streams of persons visiting venues: those who sign in manually, who could expect to be called by contact tracers to be informed of their intervention, and those would instead be 'pinged' by the app. Yet the architecture of the app meant that these were not streams with symmetric legal obligations. Those who were contacted by a call centre were legally obliged to isolate, and could face a fine if they did not. Those who were notified by

[92] Paul Garvey, 'Officials Knew WA Police Were Accessing Covid-19 Data Ahead of Election', *The Australian* (18 June 2021).
[93] Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 (Australia); Privacy Amendment (Public Health Contact Information) Act 2020 (Australia).
[94] COVID-19 (Temporary Measures) Act 2020 s 82 (Singapore). See generally Shirin Chua and Jaclyn Neo
[95] *Arrêté royal portant exécution de l'arrêté royal n° 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, 17 septembre 2020* (België).
[96] Fatina Keilani and others, 'Polizei nutzt Kontaktdaten aus Restaurants auch zur Strafverfolgung', *Der Tagesspiegel* (31 July 2020) <https://www.tagesspiegel.de/politik/faelle-aus-fuenf-bundeslaendern-bekannt-polizei-nutzt-kontaktdaten-aus-restaurants-auch-zur-strafverfolgung/26056130.html> accessed 5 November 2021; Anna-Bettina Kaiser and Roman Hensel, 'Germany: Legal Response to Covid-19' in Jeff King, Octavio Ferraz and others (eds), *Oxford Compendium of National Legal Responses to Covid-19* (OUP 2021) s VI.B.
[97] Both jurisdictions face the same structure of issues and shared a single app, whilst distinct systems operated in Scotland and Northern Ireland; I will refer only to English law for parsimony. For the Welsh situation, a starting point is The Health Protection (Coronavirus Restrictions) (No. 5) (Wales) Regulations 2020 reg 5.
[98] The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020, reg 6.

their own device had no legal obligation which stemmed from that.[99] Why was this? The architecture may hold some answers. The decentralised design of the app is such that deleting and reinstalling it would leave no trace of a notification having been given. What hope of prosecution would exist in this case without relying on the sudden seizure of a device, hugely disproportionate targeted equipment interference (hacking), or the creation of an offence of deleting the app after notification — which would somewhat remove the app's voluntary nature and itself be hard to draft in a robust and proportionate way.[100]

E. Legal and regulatory challenges to contact tracing systems

In **Norway**, a bespoke contact tracing app run by the national public health agency and developed by a governmental research agency was ordered in July 2020 to stop processing data by the Norwegian data protection authority, as it had not sufficiently established the necessity of using GPS location information, which are in general considerably more invasive than approaches using Bluetooth.[101] The public health authority deleted all data gathered using the app, and pulled its use until it was redesigned using only Bluetooth technology in a decentralised manner.[102] In **India**, challenges were raised about the data collection practices of the Aarogya Setu app. The Karnataka High Court subsequently restricted certain data sharing from the app unless informed consent was obtained.[103] In the **UK**, the English and Welsh contact tracing app was not subject to regulatory action, but the Information Commissioner at the time did tell Parliament, while there was still development of an earlier centralised app, that if she 'were to start with a blank sheet of paper, it would start with a decentralised system',[104] and to that end had previously issued a unusual, unsolicited, favourable opinion around decentralised proximity tracing.[105] In **France**, the national data protection authority (CNIL) issued an opinion on the draft decree authorising the initial centralised *StopCovid* app recommending several changes regarding, for example, user rights, the extent of logging, and potential data transfers.[106] The decree was changed in relation to this action.[107]

V. Concluding Remarks

The pandemic saw significant risk of function creep within informational infrastructures. Many were developed in a rush, and were deployed with limited evidence of efficacy. Here, I have focussed on three main areas — telecoms data, general privacy enforcement, and digital contact tracing systems. The pandemic saw significant expansion of the use of telecoms data, typically associated with the security state. In this area, states did see pressure and litigation for reform and oversight, which came with some success. Telecoms data did not become an

[99] The Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020, reg 2.
[100] See further Michael Veale, 'The English Law of QR Codes: Presence Tracing and Digital Divides' (*Lex-Atlas: Covid-19*, 25 May 2021) <https://lexatlas-c19.org/the-english-law-of-qr-codes/> accessed 5 November 2021.
[101] Datatilsynet, 'Vedtak Om Midlertidig Forbud Mot å Behandle Personopplysninger - Appen Smittestopp (20/02058-15)' (6 July 2020).
[102] Hinta Meijerink and others, 'The First GAEN-Based COVID-19 Contact Tracing App in Norway Identifies 80% of Close Contacts in "Real Life" Scenarios' [2021] medRxiv 2021.05.06.21253948.
[103] *Anivar A Arvind v Union of India* (25 January 2021) Writ Petition No 7483 of 2020 (High Court of Karnataka and Bengaluru) (India).
[104] Joint Committee on Human Rights, *Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications, HC 265* (4 May 2020) Q18.
[105] Information Commissioner's Office, 'Information Commissioner's Opinion: Apple and Google Joint Initiative on COVID-19 Contact Tracing Technology (2020/01)' (*ICO*, 17 April 2020) <https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf>.
[106] Deliberation N° 2020-056 from 25 May 2020 delivering an opinion on a draft decree relating to the mobile application known as "StopCovid" (request for opinion N° 20008032) (France)
[107] Philippe Mouron, 'Lancement de l'application StopCovid Après l'avis Positif de La CNIL' [2020] Revue européenne des médias et du numérique 5.

international pillar of pandemic response, even though there were hotspots of use. However, the pandemic did highlight states which have very little oversight over their use of such data, where vague discussions or orders were made without clear legal basis. In this regard, and particularly given the sensitivity and risk of misuse of such data for persecution or similar, the pandemic should give us pause for thought and encourage further pressure to formalise oversight of intelligence regimes.

In relation to broad privacy enforcement, we are still seeing the outcomes of this process. The world has digitised in new ways — particularly our world of work — and it is unclear that regulators have yet got to grips with all of the issues associated with this. There is some evidence to suggest a period of regulatory deference, yet it was rarely the case that privacy and data protection rights were set aside altogether. Allegations of privacy law undermining pandemic response seem inaccurate — the response appeared to coexist with these regimes in place, even if enforcement took a back seat. At the same time, such regulators had long been struggling with capacity, and they too had to adjust to remote working as well as the entirely new and frightening environment, and their effectiveness may have been impaired as a result.

Contact tracing systems presented a huge array of interesting interactions between law and computing. States had high profile, politicised computational–legal debates over the architectures of such systems. Some used this as a reason to avoid bespoke legal protections, such as when systems were decentralised, while others were forced by scandal to patch the holes created by data misuse in centralised systems. Where bespoke regimes were creates, such as in Australia, it highlighted gaps in existing patchy privacy law. Some challenges were brought to these systems, and some succeeded, but the dominance of the Apple–Google Exposure Notification system, broadly supported by civil society groups in comparison to centralised alternatives, perhaps lowered the number of these challenges.

There were a large number of informational infrastructures created in the pandemic — this chapter can focus on just a handful and their consequences. Their introduction was carefully watched. Perhaps we saw the largest politicisation of the digital that we have yet seen, with citizens engaged and considering these debates in ways they have not always done with information technologies. Given how important such infrastructures are to our daily lives, this focus should surely be welcomed — perhaps a small silver lining on a globally chaotic and traumatic time.

Acknowledgments

MV was supported in this work by the Fondation Botnar.