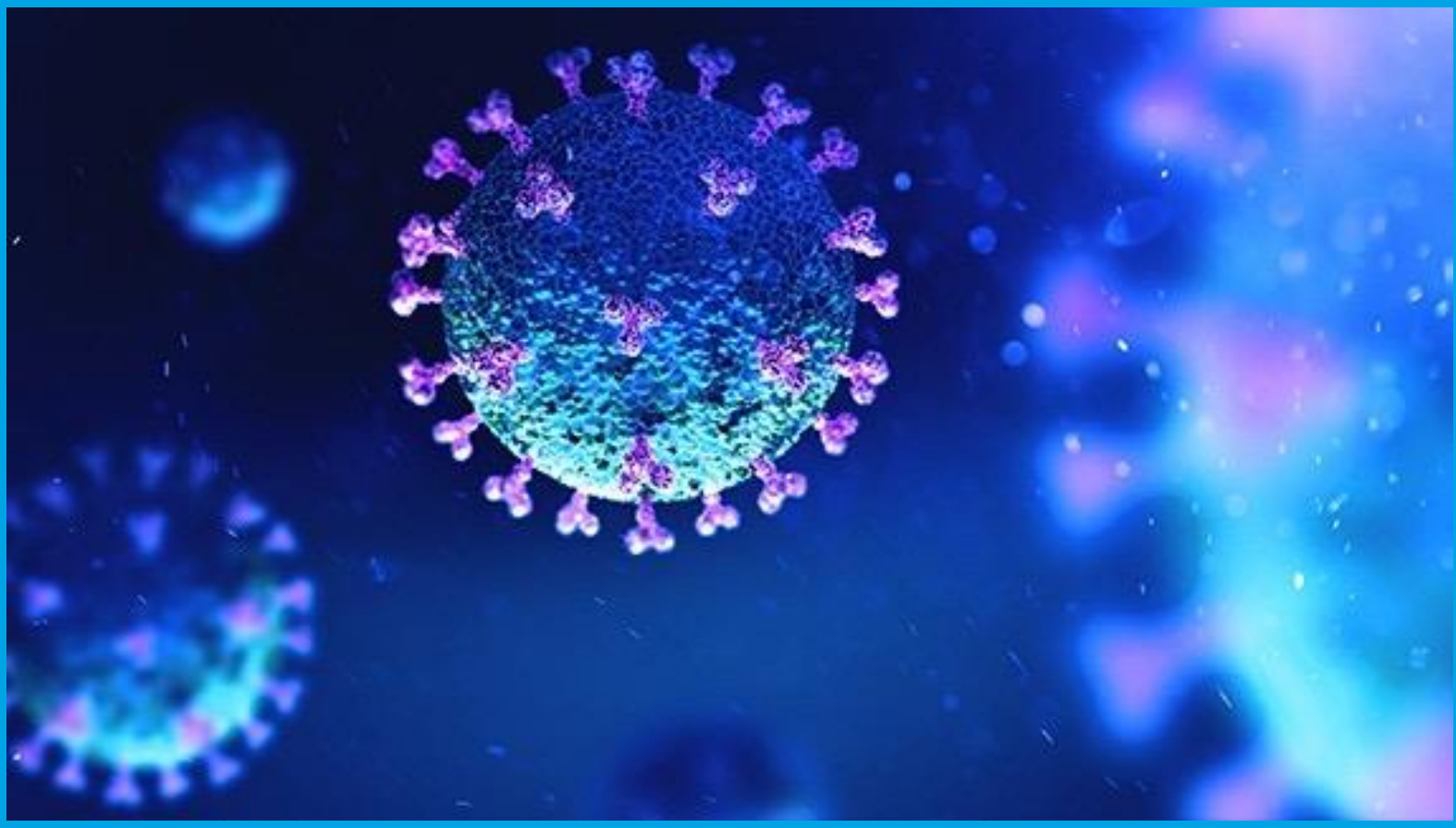
BINGHAM CENTRE FOR THE RULE OF LAW

Newcastle University

WP3-D2B 'Venue Check-In' or 'Presence' Apps

Lilian Edwards, Keri Grieman and Emma Irving



September 2021

BICL
British Institute of International and Comparative Law

The Role of Good Governance and the Rule of Law in Building Public Trust in Data-Driven Responses to Public Health Emergencies

Funded by the UK Arts and Humanities Research Council, grant AH/V015214/1

This project, at the intersection of law, ethics, citizen deliberation, public health and data science, aims to develop a distinct values-based framework to help understand and address the challenges posed by data-driven responses to public health emergencies and the need to build public trust.

In their COVID-19 responses, states have relied on data-driven approaches to justify far-reaching measures, including closing entire business sectors and categories of travel, curtailing personal liberties and requiring compliance with new technologies for contact tracing and social distancing. To be effective, such measures must be internationally co-ordinated, nationally adopted and adhered to by a high proportion of the public. Trust underpins both national adoption and public adherence: trust in international institutions, in the measures adopted, and in their scientific foundations.

This project examines two critical enablers of that trust: good governance and the rule of law. It aims to provide practical guidance on how international and national institutions can build public trust in the processes by which they design and implement data-driven responses to public health emergencies. The research consists of four interconnected work packages which examine:

(1) International governance frameworks for public health emergencies.
(2) Values-based principles to guide data-driven responses by national institutions including governments, parliaments, courts and police.
(3) UK case studies and a literature review of data governance (national and international) in relation to the use of data driven technologies in the pandemic emergency
(4) A citizen jury deliberation on the trustworthiness of data-driven measures and what additional safeguards may be needed.

https://binghamcentre.biicl.org/projects/the-role-of-good-governance-and-the-rule-of-law-in-building-public-trust-in-data-driven-responses-to-public-health-emergencies

This report forms part of Work Package 3. This work package examines how good governance and rule of law principles can help to build public trust in data-driven technologies introduced in response to public health emergencies. The work package outputs address a range of technological responses to Covid-19 by discussing the legal frameworks that govern them and identifying the issues and challenges that they give rise to from a public trust perspective. The outputs comprise:

- Rapid Evidence Response Review of Data-Driven Responses to Public Health Emergencies (WP3-D1)
- 'No jab, no job'? Employment Law and Mandatory Vaccination Requirements in the UK (WP3-D2A)
- 'Venue Check-In' or 'Presence' Apps (WP3-D2B)
- Judicial Scrutiny of COVID-19 Regulations in the UK: Addressing Deference to Data-Driven Decision-Making in Human Rights Cases (WP3-D2C)
- Policy Brief: Good Governance and Rule of Law Principles for Data-Driven Technologies in Public Health Emergencies (WP3-D3)

'Venue Check-In' or 'Presence' Apps

WP3-D2B

Main Findings

Venue check-in apps are a type of smartphone app that emerged alongside the 'contact tracing' or 'proximity' apps. Venue check-in apps focus on *presence* at a particular location or venue, to which individuals actively 'check in', and are typically aimed at public or hospitality venues. When an individual enters a venue, they scan an NHS QR code and their information is logged. In the event of an outbreak being linked to that venue, those who were there within the relevant timeframe can be notified. Following the introduction of regulations, it became mandatory for certain venues in England, Wales, and Scotland to ask visitors to check-in by providing their contact information. This could be done through the NHS provided QR codes or manually – in England and Wales, it was mandatory for venues to display NHS QR codes. Venue check-in apps gave rise to a number of good governance and rule of law concerns:

1) Transparency, legitimacy and scrutiny

- *Democratic deficit in design***.** Technical design decisions made in Scotland and England were largely not subject to any public debate and yet have significant potential to impact on privacy, autonomy, assembly and security. The absence of such debate was notable after the furore around contact tracing apps privacy in the first six months of the pandemic.
- *Deficits in public scrutiny.*
    - In both jurisdictions there was no primary legislation enabling venue check-in apps (or other Covid-19 technologies, such as vaccine passports) and little or no parliamentary oversight before issuing the apps.
    - Regulator involvement (e.g. the ICO) was largely restricted to (voluntarily submitted) scrutiny of Data Protection Impact Assessments (DPIAs).
    - In Scotland scrutiny by civil society was explicitly sought as well as that of the Scottish Human Rights Commission.
    - Public scrutiny by civil society is mainly based on impact assessments, especially DPIAs. These documents have come to fulfil a critical quasi-"freedom of information" purpose even though they were never designed for this and there is no legal requirement to publish, nor always, to create one.

2) Human rights and proportionality

- *Privacy v effectiveness for social benefit*. As with contact tracing apps, a debate exists for presence apps about whether privacy should be traded off against effectiveness. As with contact tracing apps (see WP3-D1), this expressed itself in the UK in decisions over whether to build a *centralised* system (as in Scotland) vs a *decentralised* system (as in England). There is no clear evidence these choices were data-driven, nor what objective metrics should be used to decide these kinds of balances.
- *Resources v effectiveness*. There is evidence that what primarily impeded the effectiveness of the venue check in schemes, at least at first, was resources. Public Health Authorities (PHAs) did not have the resources to send out many manual alerts that venues were loci of infection: in neither jurisdiction was alerting automated, and the reasons for this - technical, privacy-preserving and social – are unclear and need scrutiny.
- *Safeguards*. If data *is* collected centrally by Covid-19 technology, as with the Check In Scotland app, there need to be safeguards to prevent data breaches if the app is to be deemed a necessary and proportionate measure. The Scottish example gives us examples of a number of good safeguards: clear deletion schedules, encryption, control on who has access to central datastores.

- *Privacy vs digital inclusion*. Both the English and Scottish solutions took account of the risks of digital exclusion, for those without smartphones or confidence to use them, by mandating non-digital alternative means. However, the shortfalls of non-digital check-in methods mean there is a privacy trade off with inclusion.

Background

There have been a number of categories of apps developed in the COVID-19 pandemic to assist in public health goals.[1] The first and most debated type of app was the 'contact tracing app' which typically employs a variety of measures to track an individual's *proximity* to an infected individual such as to be susceptible to infection over a risky period of time (typically, within two metres distance, over 15 minutes time). This proximity tracking may or may not involve also recording the user's location and/or other personal data.

In the various jurisdictions of the UK and in much of the EU and US, there was a notable and heated debate over the privacy impacts of such technologies, and fears of the state surveillance potential, possibly extending beyond the pandemic.[2] After much debate, a privacy preserving, decentralised, proximity protocol was developed for contact tracing apps (GAEN or Google Apple Emission Notifications[3]), with uptake driven by the control Google and Apple have over smartphone infrastructure. This protocol could be implemented in different national apps. GAEN based apps do not record the user's location or identity in any central database. Instead, on a user's phone, the app risk-assesses proximity to an infected person over a period of time, and sends alerts or 'pings' if there has been a risky level of proximity.

A second type of app has emerged alongside the above which focuses on *presence* at a particular location or venue, to which individuals actively 'check in'. Such functions are typically focused on public or hospitality venues. We can label these *presence* rather than *proximity* tracing apps.[4] Again, these apps can be coded in ways which are less or more privacy preserving,[5] although there seemed anecdotally to be far less debate about this type of app compared to *proximity* apps, at least in the UK.

The basic objective behind asking individuals to check into a location is to limit the spread of Covid-19 by alerting individuals who may have been exposed to a virus at a given location. When an individual who attended a venue tests positive, those who shared time at a venue with them can be informed that they might be at risk. In some jurisdictions this information might be accompanied by an obligation to isolate, and/or get tested; in others it might simply be informational.

---

[1] See Rapid Evidence Review of Data-Driven Responses to Public Health Emergencies, WP3-D1 (September 2021)

[2] Lilian Edwards, 'Apps, Politics, and Power: Protecting Rights With Legal and Software Code' in Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press, 2020), 40-42

[3] 'Exposure Notification' (*Apple*) <https://developer.apple.com/exposure-notification/> accessed 16 September 2021. Note the protocol was partly based on work done by a non-profit academic EU consortium, DP3T. See discussion in Michael Veale, 'Sovereignty, Privacy and Contact Tracing Protocols' in Taylor et al (*supra* n2), 35-39.

[4] Term created by Michael Veale in 'The English Law of QR Codes: Presence Tracing and Digital Divides' (*Lex Atlas*, 25 March 2021) <https://lexatlas-c19.org/the-english-law-of-qr-codes/> accessed 16 September 2021

[5] For example Hong Kong's LeaveHomeSafe app and Singapore's Trace Together app both provided venue check in functionality but with an unclear degree of privacy protection: see eg Gerard Goggin, 'COVID-19 apps in Singapore and Australia: reimagining healthy nations with digital technology' [2020] 177(1) Media International Australia 61–75; and Michelle Chan, 'Hong Kong residents find ways around mandatory contact tracing' (*NikkeiAsia*, 23 February 2021) <https://asia.nikkei.com/Spotlight/Coronavirus/Hong-Kong-residents-find-ways-around-mandatory-contact-tracing> accessed 6 October 2021

This case study focuses on presence-tracking apps, examining the English/Welsh 'NHS Covid-19' app and the Scottish 'Check In Scotland' app. The NHS Covid-19 app has a proximity tracking function as well as a check-in function, but only the latter is examined in this case study. Both apps use the same basic functionality of QR codes displayed at venues allowing users to 'check in'. Interestingly, different choices were made in England and Wales compared to Scotland when it came to the architecture and legal implementation of the apps, with different effects for privacy, transparency, human rights and, arguably, public trust.

Key English-Welsh/Scottish Distinctions

- Legal mandate and timescale. Prior to 19 July 2021 visitors to certain types of venues in England and Wales were legally required to check in, either through the NHS Covid-19 app or by leaving their details manually.[6] This requirement has now ended, although checking in is still strongly encouraged.[7] In Scotland, as of 9 August 2021, a similar legal requirement *remains* on venues in certain sectors to collect contact details from visitors.[8]
- Integration. In England a deliberate choice was made to incorporate the check-in functionality into the national contact tracing app ('NHS Covid-19 app')[9] probably as a (successful) means to drive uptake of the proximity app. In Scotland the presence app ('Check In Scotland') was coded separately from the contact tracing app ('ProtectScotland').
- Architecture and Privacy. In England a decentralised privacy preserving architecture was specified, as with the parent contact tracing app, while in Scotland a more centralised, less privacy preserving architecture was chosen, where check in data is stored centrally for up to 21 days albeit with strong safeguards. Scotland was able to adopt this approach because, by not incorporating their presence app into their GAEN-protocol contact tracing app, they were not bound by Google and Apple's privacy policies.

How the Apps Work

1) England and Wales

Users 'check in' using the NHS Covid-19 app by scanning the venue's QR code: the time and date of their arrival is recorded in the app, on the user's phone. All members of a party entering a venue are encouraged to check in, provided they are 16 or over.[10] Users do not need to check out of a venue when leaving, but will be checked out automatically when they check in elsewhere or after midnight.[11] QR codes are displayed on official NHS posters that display the NHS Test and Trace or the NHS Wales

[6] Section 7, The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020
[7] NHS COVID-19 app support, 'Common Questions' <https://faq.covid19.nhs.uk/article/KA-01137/en-us?parentid=CAT-01035&rootid=CAT-01032> accessed 16 September 2021
[8] Scottish Government, News, 'Scotland to move beyond level 0' (3 August 2021) <https://www.gov.scot/news/scotland-to-move-beyond-level-0/> accessed 16 September 2021
[9] Not to be confused with the 'NHS App' which pre pandemic was used as an online way to retrieve medical records, book appointments, etc. and has during the pandemic been repurposed as a 'vaccine passport'. (NHS, 'NHS COVID Pass' < https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/> accessed 16 September 2021)
[10] Department of Health and Social Care, 'Guidance: Maintaining records of staff, customers and visitors to support NHS Test and Trace' (20 July 2021) <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> accessed 16 September 2021
[11] NHS COVID-19 app support, 'Common Questions' <https://faq.covid19.nhs.uk/article/KA-01134/en-us?parentid=CAT-01035&rootid=> accessed 16 September 2021

Test, Trace, Protect logo.[12] Venues that can display these posters include hospitality, tourism and leisure services; services involving close contact such as hairdressing; and community centres, village halls, and libraries.[13]

Decentralised System

The app for England and Wales operates in a privacy preserving decentralised way, meaning that the record of venues visited is stored on the user's own phone. A Public Health Authority (PHA) may manually make a determination, from public health information, that a venue is a locus of infection. It can then issue an identifier of the venue to individual phones, where a comparison and match can be made. If a match is made, the user will receive an alert informing them that they need to watch for symptoms or book a test. The name of the venue is not included and there is no central PHA or government record of the match. The app communicates with the central system every 2 hours to check for matches.[14] The venue history stored on the phone is deleted automatically after 21 days.[15] The effect is that the user is warned that they may have been somewhere risky but no data about their movements is stored centrally. This is very privacy sensitive and therefore arguably good for trust.

The downside is that the PHA cannot monitor whether contacted users do get a test or isolate, and in this sense, it is identical to the privacy preserving contact tracing (proximity) app. Furthermore, as with contact tracing apps, the privacy preserving architecture means that the user receives very little information, which may influence their choice to get tested, isolate or take other action. They do not know which venue has generated the match (though they may have an educated guess) just as users of the contact tracing app often complain that they don't know where they were near an infected person to generate a 'ping', nor who it was. Such lack of an underlying 'narrative' may partly dissuade those notified from using the information they are given.

In April 2021, the government sought to introduce a radical change whereby users would be asked to opt in to sharing their venue check in data with a *central system*. This would have allowed, the government said, for venue-related alerts to be automated, instead of relying only on authorities to manually flag a venue.[16] The update was halted by Apple and Google on the basis that it violated their privacy policy for contact tracing apps, which are explicitly not allowed to collect the location data

The Legal Framework

The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020 placed an obligation on the person in charge of a venue to collect the contact details of visitors to that venue. Venues were obliged to display an official NHS QR code to facilitate digital check-in through the NHS Covid-19 app, but visitors could leave their details manually if they preferred. If visitors refused to provide their details, the venue was obliged to refuse entry. Failing to collect contact details and display a QR code were offences under the Regulations. As of 19 July 2021, these regulations were revoked and the obligations no longer apply.

[12] NHS COVID-19 app support, 'Common Questions' <https://faq.covid19.nhs.uk/article/KA-01135/en-us> accessed 16 September 2021
[13] NHS COVID-19 app support, 'Common Questions' <https://faq.covid19.nhs.uk/article/KA-01183/en-us?parentid=CAT-01043&rootid=CAT-01027> accessed 16 September 2021
[14] Department of Health and Social Care, 'Guidance: NHS COVID-19 app: anonymisation, definitions and user data journeys' (3 September 2021) <https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys> accessed 16 September 2021
[15] NHS COVID-19 app support, 'Common Questions', <https://faq.covid19.nhs.uk/article/KA-01213/en-us> accessed 16 September 2021
[16] Leo Kelion, 'NHS Covid-19 app update blocked for breaking Apple and Google's rules', BBC News (12 April 2021) <https://www.bbc.com/news/technology-56713017> accessed 16 September 2021

of users to a central store (see above).[17] As the England and Wales venue check-in function was built into the contact tracing (proximity) app, this policy applied to the check-in function too.

Automation would seemingly be useful because, according to reports from Sky News in March 2021, the ability to send out messages to users about a risky venue was in fact barely used. This was because the system imposed a 'significant administrative burden' on stretched local health protection teams, who had to make this call manually, and many of which were also unclear about how or when to tell Test and Trace about a risky venue.[18] Arguably 'the failure of the £22bn service to use the data for alerts or contact tracing meant "thousands of people" were not warned they might be at risk of infection'[19] and showed a lack of integration between public health, and Test & Trace (another familiar theme from the early days of the pandemic).

Statistics on the operation of the English presence app have been collected by a private party at https://russss.github.io/covidtracker/app.html. After a slow start they show that almost 10,000 venue risk alerts were sent out between the launch in September 2020 and August 2021, although significant numbers of alerts only really happened in July 2021. Around this time infections were rising after lockdown had eased, and a short time later on 19 July 2021 the system ceased to be mandatory, though the service is still offered a voluntary basis and for users to check-in using their app.

2) Scotland

Check In Scotland can be downloaded on a smartphone from the Apple and Google app stores and can be used by anyone over the age of 12.[20] To check in, an individual scans the venue's QR code with the camera on their phone, or with a QR code scanning app. This takes users either to an online form where they can fill in their contact information, or if the app is already installed on their phone, they are directed

The Legal Framework

Health Protection (Coronavirus) (Requirements) (Scotland) Regulations 2021 placed an obligation on those in charge of venues to take measures to collect contact information from visitors spending time at the venue. Failing to do so constituted an offence. There was no obligation to display a QR code, and no stipulation as to whether the information should be collected manually or digitally. Venues were not required to refuse entry to visitors who refused to provide their contact details. As of September 2021, these regulations were still in force.

[17] *Ibid*
[18] Rowland Manthorpe, 'COVID-19: Test and Trace barely used check-in data from pubs and restaurants – with thousands not warned of infection risk', Sky News (4 March 2021) <https://news.sky.com/story/test-and-trace-barely-used-check-in-data-from-pubs-and-restaurants-with-thousands-not-warned-of-infection-risk-12235392> accessed 16 September 2021
[19] *Ibid*
[20] 'How to use the Check In Scotland QR code' (9 August 2021) <https://www.mygov.scot/help-qr-check-in> accessed 16 September 2021

to the app to check in.[21] If the phone is not able to scan the QR code, there is a short form URL on the poster that can be put into a phone's web browser.[22] When leaving a venue, individuals should check out - by using the same webpage a person checked in with, rescanning the QR code, or through the app.[23]

QR codes are displayed on official Check In Scotland Test and Protect posters. Pubs, bars, restaurants and cafés are obliged to collect and record visitor information, through the app or manually. Other venues can do so optionally, including theme parks, museums, hairdressers, libraries, burial authorities, and places of worship.[24]

The Check In Scotland app works in conjunction with NHS Scotland's Test and Protect service. When contact tracers see that a person has been at the same venue at the same time as someone who has tested positive for corona virus, as in England, they can manually issue an alert, using contact information provided during check in. The alert may require a person to watch out for symptoms, book a test, or self-isolate.[25] In Scotland, requirements to self-isolate are never legally binding. The decision to issue an alert is not automated, and always involves human input.[26]

Statistics have not been made public in Scotland concerning the number of check-ins or the number of venue alerts sent out. A request was made for such statistics but has not so far had a reply.

Centralised System

Contact tracers can see whether a person was at a venue at the same time as someone who has tested positive because the Check In Scotland app works in a centralised way. When a user fills in their contact information after scanning a QR code, the data is stored in a central, secure database that can be accessed in response to a Covid-19 outbreak.

The DPIA released alongside the app sets out the reasons for opting for a centralised design in Scotland, unlike the decentralised option in England:

- Using a centralised system reduces the risk of loss of data, perhaps due to users deleting data on their phones because they seek to avoid isolation or venues seeking to avoid being closed down. In the England and Wales model, individuals and venues can delete venue visit data, and may do so before the Test and Protect teams can contact visitors and inform them of a risk of infection.[27] By holding the data in a centralised store, it is accessible to the Test and Protect teams for 21 days and can be used to help break the transmission of Covid-19 more effectively. The possibility of automating alerts – which was cited as a reason behind the failed move to centralised in the England and Wales app – is *not* mentioned as an advantage of the centralised model. Indeed, the DPIA stresses that a human is always involved in the decision to issue an alert.[28]

---

[21] *Ibid*
[22] *Ibid*
[23] *Ibid*
[24] 'Create a Check In Scotland QR code poster' (30 June 2021) <https://www.mygov.scot/qr-check-in> accessed 16 September 2021
[25] 'How to use the Check In Scotland QR code' (*supra* n20)
[26] NHS Scotland Test&Protect, 'The Check In Scotland digital service: Data Protection Impact Assessment' (20 April 2021), 30
[27] *Ibid*, 84
[28] *Ibid*, 30

- It allowed the Test and Protect teams to contact at risk individuals, rather than relying on their phones to issue an alert. The DPIA does not explicitly clarify the advantage of this more direct contact.[29]
- Venues must 'take measures' by law to collect visitor information (see 'legal framework' above), and the DPIA asserts that if data could be deleted from a phone using a decentralised app, this data would not then be available for the purpose of contact tracing.[30] Thus it was argued a more decentralised design would have been at odds with the law. This seems a stretched interpretation; a venue would already have 'taken measures' even if users later behaved anti-socially.

The DPIA acknowledges that a centralised system is uncomfortable from a privacy point of view, and indicates that the public's negative perception of this approach was taken into account during the decision making.[31] Safeguards were put in place however to make the approach necessary and proportionate.[32] These included:

- Data retention – Data is deleted from the central database after 21 days.[33]
- Access to data – Data can only be accessed by a member of the Health Board's contact tracing team or person authorised by a relevant Director of Public Health. The access needs to be approved by senior management in both NHS National Services Scotland and Public Health Scotland.[34] There is no other way for data to be released.
- Encryption – All data is encrypted, with personal data such as name, phone number, and address being double encrypted.[35]

The DPIA was explicitly signed off on by a relevant civil society organisation - the Open Rights Group - as well as the Information Commissioner's Office (ICO) and a focus group from the Scottish Children's Parliament. The 'digital ethics' were also discussed by the Scottish Privacy Forum, the NHS Scotland Public Benefit and Privacy Panel, and the ICO. This explicit commitment to audit concerning rights, especially privacy and discrimination, was rather different from the pattern in England when apps were built during the pandemic (see WP3 D2-A discussion on vaccine passports). The GDPR does not always require publication of DPIAs (art 35) but it has become seen as good practice for technology of public importance developed by the state.

Key Good Governance and Rule of Law Concerns

1) Privacy

Technology that tracks where a user has been and who they have been in contact with will inevitably raise privacy concerns. Steps were taken to overcome these concerns by building privacy protective features into the design of the venue check-in apps for England and Wales and Scotland.

[29] *Ibid*, 85
[30] *Ibid*, 87
[31] *Ibid*, 85
[32] *Ibid*, 88
[33] See 'Check In Scotland Privacy Policy' (18 December 2020) <https://www.mygov.scot/check-in-scotland-privacy-policy-venues> accessed 16 September 2021
[34] Check In Scotland DPIA (*supra* n26), 23, 29
[35] *Ibid,* 29

The decentralised design of the NHS Covid-19 app for England and Wales only stores personal data on the phone itself, and any data that is shared is anonymised. In light of this, it is not clear whether the data collected would even fall under the GDPR as it may not count as personal data.[36] Additional privacy measures include traffic-based obfuscation (preventing inferences from traffic patterns), no GPS interaction, and no IP address collection.[37] While the Check In Scotland app does share personal data with a central system (name, phone number, email), it uses double encryption and strict access protocols to protect the data (see above). Both Check In Scotland and NHS Covid-19 apps have data retention rules that require the data to be deleted from either the central store or the phone after 21 days.

Thanks to these design features, checking in by scanning a QR code using one of these apps (or the associated web page version for Check In Scotland) is often more privacy protective than checking in using either a manual sign-in sheet or a private sector QR code. Women have been harassed by calls from people who had collected their contact information from sign-in sheets, including staff of the venue they had visited.[38] Bars and pubs that have developed their own QR code check-in service, separate from the NHS system, have at times used the data collected for marketing purposes.[39] This has prompted calls for the government to set out rules on how this data should be handled by private companies.[40]

Having one state-sponsored system of QR code check-in has the additional benefit of reducing the chance of users scanning malicious QR codes. For users in England and Wales, QR codes must be scanned from within the NHS Covid-19 app, and non-official codes will not work.[41] This is more problematic with the Scottish app, where users can scan a QR code with their phone camera and so are not similarly protected.[42]

Privacy related barriers for trust still remain however. The dispute between Google and Apple and the English government over the update to the NHS Covid-19 app gave the impression that the technology companies were more protective of user's privacy than the authorities. The update would have allowed users to opt in to sharing their venue check-in data with a centralised system, and was blocked by Google and Apple. The Scottish app has been criticised for using a centralised system, which raises

[36] Christiane Wendehorst, 'COVID-19 Apps and Data Protection' in Ewoud Hondius, Marta Santos Silva, Andrea Nicolussi, Pablo Salvador Coderch, Christiane Wendehorst, and Fryderyk Zoll (eds), *Coronavirus and the Law in Europe* (Intersentia, 2021) (freely available at <https://www.intersentiaonline.com/library/coronavirus-and-the-law-in-europe> accessed 15 September 2021).
[37] Mark Briers, Chris Holmes, and Christopher Fraser, 'Demonstrating the impact of the NHS COVID-19 app: Statistical analysis from researchers supporting the development of the NHS COVID-19 app' (*The Alan Turing Institute,* 9 February 2021) <https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app> accessed 16 September 2021
[38] Beth Hale, 'Has Test and Trace become a stalker's charter? Giving your mobile number to a bar or restaurant is supposed to keep you safe but women are reporting troubling stories of texts from strangers and even harassment', The Daily Mail (7 October 2020) <https://www.dailymail.co.uk/femail/article-8815891/Women-reporting-troubling-stories-texts-strangers-used-test-trace-details.html> accessed 16 September 2021
[39] Shanti Das and Shingi Mararike, 'Contact-tracing data harvested from pubs and restaurants being sold on', The Times (11 October 2020) <https://www.thetimes.co.uk/article/contact-tracing-data-harvested-from-pubs-and-restaurants-being-sold-on-s0d85mkrr> accessed 16 September 2021
[40] Jim Killock, 'NHS App Users Get Privacy; Other Visitors Get Nothing' (*Open Rights Group,* 24 September 2020) <https://www.openrightsgroup.org/blog/nhs-app-users-get-privacy-other-visitors-get-nothing/> accessed 16 September 2021
[41] NHS COVID-19 app support, 'Common Questions', < https://faq.covid19.nhs.uk/article/KA-01133/en-us?parentid=CAT-01035&rootid=> accessed 16 September 2021
[42] 'How to use the Check In Scotland QR code' (*supra* n20)

concerns of government surveillance.[43] The DPIA for Check In Scotland does not rule out the possibility of the data being used for police purposes, if certain requirements were met.[44]

2) Inclusion and Equality

From an inclusivity point of view, it is positive that the England and Wales NHS Covid-19 app is available in 12 languages (and less positive that the Scottish app is available in English only). It is also positive that venues continue to offer alternatives to digital check-in for those who do not have access to a smartphone or do not possess the digital literacy or inclination to use one. That being said, for the availability of paper-based manual check-in to be an equal alternative to digital check-in, solutions must be found for the privacy problems identified above.

The key difference between manual check-in and digital check-in is, however, in the consequences in case of an alert. When a user of the England and Wales NHS Covid-19 app receives an alert that they may have been exposed to Covid-19, they are not legally obliged to self-isolate. This is different if they are contacted directly by a Test and Trace official, where such an obligation can be imposed. This means that an individual who checks-in to a venue with a QR code, and whose presence at that venue is recorded only on their phone, may be subject to a lesser restriction than someone who checked in manually and who was contacted by a Test and Trace official.[45]

With the Scottish app users are always contacted by a Test and Protect official, and so this difference does not exist.

3) Democracy and Accountability

In England, the obligation on venues to collect visitor information was brought into effect by means of regulations[46] enacted under the Public Health (Control of Disease) Act 1984. Regulations were used, rather than primary legislation, because of the perceived urgency of the situation; however, this means that they were not laid before and approved by Parliament. Some debate did take place in the House of Lords, where points relating to privacy and surveillance were raised,[47] but there appears to have been little or no debate in the House of Commons to date. The absence of such debate, both in Parliament and in the public space more generally, was notable after the furore around contact tracing apps privacy in the first six months of the pandemic. Alongside this deficit in parliamentary scrutiny was a lack of regulatory scrutiny. Regulatory involvement (for example from ICO) was largely restricted to (voluntary) scrutiny of impact assessments. The regulations have now been revoked.

In Scotland the obligation to collect visitor information was also enacted in regulations,[48] in this case using powers in the Coronavirus Act 2020. Similarly, they were not laid before the Scottish Parliament for approval before being passed, and in this case there appears to be no record of parliamentary debate. Input from civil society and actors such as the Scottish Human Rights Commission was, however, explicitly sought for the Check in Scotland app during the development process.

Public scrutiny of both check-in apps has been largely based on the DPIAs published by the English and Welsh and Scottish authorities. These documents have come to fulfil a freedom of information

[43] Michael Hill, 'Privacy Concern Over Scotland's New #COVID19 Check-In App' (*infosecurity,* 7 April 2021) <https://www.infosecurity-magazine.com/news/privacy-covid19-checkin-app/> accessed 16 September 2021
[44] Check In Scotland DPIA (*supra* n26), 79
[45] Michael Veale, 'The English Law of QR Codes: Presence Tracing and Digital Divides' (*Lex Atlas,* 25 May 2021) < https://lexatlas-c19.org/the-english-law-of-qr-codes/> accessed 16 September 2021
[46] Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020
[47] HL Deb 7 October 2020, vol 806
[48] Health Protection (Coronavirus) (Requirements) (Scotland) Regulations 2021

purpose, even though the purpose of impact assessments is to reduce the risk for the data controller, rather than the public. There is no legal requirement to publish a DPIA, and while it may be questioned whether this is the best way to manage public transparency and scrutiny, they have been an important way to communicate information about the technology.

BINGHAM CENTRE FOR THE RULE OF LAW

Newcastle University

Charles Clore House
17 Russell Square
London WC1B 5JP

T 020 7862 5151
F 020 7862 5152
E binghamcentre@biicl.org

www.binghamcentre.biicl.org

The Bingham Centre for the Rule of Law is a constituent part of the British Institute of International and Comparative Law (www.biicl.org).

Registered Charity No. 209425

BIICL

British Institute of International and Comparative Law