Privacy & Pandemics: The Role of Mobile Apps (Chart)

Apps and Software Development Kits Compared:
K Health (US), HaMagen (Israel), TraceTogether (Singapore), COVID Symptom Tracker (UK), Home Quarantine (Poland), and Decentralized Privacy-Preserving Proximity Tracing (DP-3T) (EU)

The apps and software development kits (SDK) compared below have been deployed to help tackle the COVID-19 pandemic, which poses a major threat for countries around the world. Their specific objectives and methods diverge significantly. Two were developed by private entities for the purposes of digital health management and research, respectively. The others were developed by international initiatives and governments - for the purposes of contact tracing, infection tracking, and quarantine compliance. A key commonality between them is their use of sensitive personal information, namely health-related information and/or location information. The chart compares relevant privacy and data protection issues - such as data collection, retention, purpose, and sharing - as well as what privacy and data security safeguards are employed. We make some general observations about effectiveness, proportionality, and compliance with fundamental human rights. The key question is how to appropriately and ethically balance public health & safety with privacy risks and other interferences with civil liberties throughout the crisis and in the future.

To meet their objectives, many of these apps and SDK's depend on mass adoption to maximise network effects. This requires public trust at a time when the public is wary about government and private data collection, use, and sharing. Mechanisms that rely on location tracking may be met with criticism in terms of surveillance and diminished privacy expectations, especially in jurisdictions that lack adequate data protection frameworks. Location data is challenging to fully anonymize. Even apps that collect aggregated location data to reveal general trends and risks at the macro level for research purposes (e.g., the COVID Symptom Tracker) may inadvertently reveal sensitive personal information if necessary precautions are not taken.

For those seeking to identify precise user location or relative proximity, effectiveness varies depending on the method used. HaMagen collects user GPS location, PEPP-PT and TraceTogether approximate user location using Bluetooth, and Home Quarantine combines GPS location with facial recognition technology. By identifying relative proximity to others, rather than exact location, Bluetooth is typically less privacy-invasive than GPS. It may also be more effective, especially inside large buildings and in urban areas. The accuracy of GPS signals varies widely, and can be affected by weather or physical interference. Apps that rely on symptom self-reporting may suffer from data accuracy and completeness limitations (e.g., K Health and COVID Symptom Tracker). These problems may be mitigated by employing AI/ML models, which can improve over time by inputting additional aggregated and anonymized user data. An overarching limitation of all of the software compared is that older citizens - the demographic population most vulnerable to COVID-19 - often do not have smartphones or do not always carry smart phones with them.

	K Health App	HaMagen App	TraceTogether App	COVID Symptom Tracker App	Home Quarantine App	DP-3T SDK
Software Purpose	**General digital health management App** with newly added COVID-19 features (risk assessments, symptom heatmap, local testing center information, and virtual primary care).	**Contact tracing App** to alert users to possible exposure to COVID-19 quickly (examines user movement - dates, times, and locations - in relation to identified patients).	**Contact tracing App** to inform users if they were in prolonged proximity to persons infected with COVID-19 (using Bluetooth to identify relative proximity in a decentralized manner).	**Research App** aiming to help scientists understand COVID-19, and to eventually help the NHS to support sick individuals. The questions may evolve as more is learned about the virus.	**Quarantine compliance App** to enable authorities to handle the mandatory quarantine of individuals (e.g. location tracking, health assessment, notifications & provision of needed items).	**Open-source software for an internationally applicable proximity tracking mechanism** which interrupts new chains of COVID-19 transmissions & alerts users who have been in close proximity with infected individuals.
App creator	Private entity.	Government.	Government.	Private entity.	Government.	International researchers.
Scope of personal data collected	"Health" data (e.g., symptoms and medical history); "other" data (e.g., age, gender, contact info, name, location, IP address); & "non-personal" data (e.g., browsing activities).	Movement and location information.	Phone number and a randomly generated anonymized User ID associated with the phone number of users within 6.5 feet of one another for 30 minutes. It does **not** track users' location.	"Sensitive" data (e.g. health data, IP address, and location); "other" personal data (i.e., contact information - email address required).	Citizen ID, full name, telephone number, quarantine location information, actual GPS location, photo of face, device photos, requested food & psychological help.	The anonymous ID of each user who is in epidemiologically sufficient proximity to a user infected with COVID-19 for an epidemiologically sufficient period of time.
How personal data is collected	Via individuals (account creation or contacting the App); via third party Apps; and via third party tracking tech (cookies, beacons, tags, pixels etc).	Collected from the time of installation of the App. Future versions may receive location history from Google (with consent).	Phone number is self-provided. When users are proximate to one another, the phones use Bluetooth to exchange Temp ID's with one another.	Self-reported and collected through default permission settings.	Self-uploaded geo-located face photos within 20 minutes of request; phone number required to register. Extensive device permissions enabled.	Users broadcast Temp authenticated & anonymous ID (can't be connected to them). Relative proximity estimated using radio signals (Bluetooth, etc).

Who can access the data	Employees, service providers, affiliated doctors, and law enforcement. It is never disclosed to third parties without consent.	If transferred to the Ministry of Health with consent, it may only be accessed by employees, representatives, and service providers.	If a user becomes infected, they have the option to give a trusted public health authority access to their App data. This may be required.	"Sensitive" data is shared with health researchers (i.e., hospital workers, the NHS, universities, health charities, other research institutions).	The Ministries of Health and Digital Affairs; Police; voivods; central IT center; Take Task S.A; Center of Health Information Systems.	Not accessible to anyone. If a user tests positive, they may voluntarily provide data to national trusts in order to notify relevant users.
Purposes the data is used for	To provide health information; improve AI models; operate & customize services; contact individuals; and for other legitimate interests. "Non-personal" data may be used at the providers discretion.	To create a detailed history of the places a user visits and the dates and times of such visits. This is cross referenced for overlap with data from COVID-19 patients to help identify people who should isolate.	Strictly to perform contact tracing. Once contact tracing ceases, users will be prompted to disable the functionality of the App.	To advance scientific research to better understand COVID-19; to identify high-risk areas; and the links between patients' health and their response to infection; and to help the NHS support sick individuals.	To support authorities to monitor quarantine compliance and epidemiological supervision of persons suspected of being infected with COVID-19.	For contact tracing to alert users in close enough proximity to infected users who create an exposure risk. If a user becomes infected, the App alerts others who have been around them in the preceding days.
Where the data is stored	Any country in which the App or their affiliates maintain facilities.	Internal memory of user cellular devices. May be transferred to the MOH.	Proximity data stored on user devices. Other data stored in a secure server.	Any country in which the App or their affiliates maintain facilities.	Government servers.	Recorded in the encrypted proximity history stored locally on the device.
How long is the data stored?	As long as necessary to comply with legal obligations, to enforce agreements, and to protect legitimate interests. Users may request erasure of personal data.	Deleted upon removal of the App from the device.	Records of encounters are stored for 21 days on device. If consent is revoked, mobile number and User ID is deleted, so data exchanged with other phones is no longer associated with the user.	Sensitive data is retained for "no longer than necessary." Individuals may withdraw consent. Other personal information is kept for no longer than 6 years after the last communication.	The registration selfie is stored for up to 6 years after deactivation of the App. Other data stored by the App will be deleted when the individual's quarantine ends.	Temporarily. Older events in the proximity history are deleted when they become "epidemiologically unimportant."

Effectiveness	The more specific information is shared about an individuals' symptoms, the more accurate and relevant information provided is. Accurate self-reporting relies on trusting users to report consistently.	Possible technical limitations may reduce the accuracy or completeness of the data. The accuracy of GPS signals may be reduced by weather or physical interference. Widespread downloads necessary to be effective.	Bluetooth may be more effective to determine proximate locations than GPS. May be disabled by turning off Bluetooth permissions or deletion. Data accuracy & completeness limitations. Widespread downloads necessary.	Reliance on crowd sourced self-reporting has debatable utility and effectiveness. It relies on trusting users to report symptoms accurately and consistently. Some accessibility and functionality issues.	Promotes compliance with mandatory quarantine. However, the user is responsible for the accuracy of the data provided and for installing security updates. There have been some reports of bugs and redundant police visits.	Scalable and open, and can be used by any country. The backend services can deal with hundreds of millions of registered devices. Use of Bluetooth for contact tracing is relatively effective. The approach promotes high downloads internationally.
Proportionality, fundamental rights, and data protection & privacy issues	"Non-personal" data, which may be used and shared by the App provider at its discretion, is defined as information that cannot be traced back to an individual e.g. information relating to browsing activities, user device, operating system, internet browser.	Data collected is claimed to be "necessary to fulfil the Apps' goals." Critics have concerns about Government surveillance. Users may receive alerts requiring them to enter home isolation. Because data is stored on users' devices, they have no claim for privacy violations as a result of usage.	There are guarantees that data will be used strictly for contact tracing. Persons diagnosed with COVID-19 are required by law to assist MOH to accurately map their movements and interactions. As location data is not collected, concerns about Government surveillance are somewhat mitigated.	The legal basis for processing sensitive data is consent, and legitimate interests is the basis for processing other data. Data may be exported to countries outside of the EU with less stringent data protection rules. The App was released with default permission settings. It does not use all of the permissions.	Processing is justified by important public interest. People may choose between installing the App or police visits. Users are required to immediately notify authorities if they develop symptoms. Non-compliance with obligations may result in legal coercion. The Privacy Policy is not easily accessible or translatable.	Striking the appropriate balance between public health and safety while maintaining high standards of privacy is central to the project. A central principle driving the work forward is to "not allow a health crisis to lead to a weakening of privacy that so many generations before us have fought for."
Privacy safeguards	The App is opt-in. High data security standards, training and internal policies,	The App is opt-in. The MOH shall "make every effort" to maintain adequate	The App is opt-in. A privacy preserving method used - Temp ID is generated by	The App is opt-in. When personal data is shared, an anonymous code	The App is technically opt-in. However, there are reports of accounts being	The App is opt-in. The code embeds safeguards to encrypt data and anonymize

	purpose specification and retention limitations. Users also have the option to use the App anonymously by choosing any username.	information security in accordance with the sensitive nature of the information" (GPS location). The open-source nature of the code promotes security, transparency, and privacy.	Bluetooth by encrypting the User ID with a private key held by the MOH. The ID is refreshed regularly (no persistent identifier) and stored on device. Bluetooth is less privacy invasive than GPS.	replaces personal details. Third party processors are contractually prohibited from using data for their own purposes or retaining it. Data security best practices are enforced.	automatically created for some people. The administrator has appointed a Data Protection Officer who can be contacted in matters relating to personal data processing.	personal information. This makes it virtually impossible to reveal the identity of the people using the devices. Users' aliases are changed frequently (rotation of the ID) and the code is frequently inspected by experts.
Open source	No.	Yes.	Yes.	Forthcoming.	No.	Yes.
AI/MI claims	Yes. Natural language processing, natural language understanding, classification and clustering algorithms techniques.	None described.	None described.	None explicitly described, major partner uses advanced regression techniques.	No facial recognition - relies instead on facial detection and image classification innate in users phones.	Claim to have input from artificial intelligence experts. Algorithms are used to measure user proximity between users with radio signals (e.g. Bluetooth).
Privacy Policy	Yes: click here	Yes: click here	Yes: click here	Yes: click here.	Yes: accessible as a download in Polish.	Reference implementation flow

K Health App (US)

To tackle COVID-19, new features have been added to this general digital health management App (e.g. risk assessments, symptom heatmap, local testing centers, and virtual primary care). The App may collect a multitude of personal information. Users may choose an anonymous username to create an account. Personal information is not sold or shared with third parties (aside from service providers), and is subject to purpose limitations and retention limitations (subject to legitimate interests). The App intends to be "at the forefront of data privacy and protection." AI models are used to provide services. Privacy Policy: click here.

Who built the App?	**Private company.** "The App was built by hundreds of expert doctors and scientists."
Intentions and capabilities	A telehealth App designed to provide people with free access to relevant healthcare through digital management of primary healthcare. This covers not only COVID-19, but also other physical and mental conditions. (i.e. the provision of health information, diagnosis, virtual connection between patients and doctors, provision of tests and prescriptions). To tackle COVID-19: new risk assessment tool, symptom heatmap, and a "testing centers near me" section, and free virtual primary care from doctors for coronavirus questions and symptoms.
What data is collected?	Users must share symptoms, age and gender. Additional data may also be collected, e.g., health data: illness, potential causes, medical history, test results, other personal data: name, phone number, DOB , location, IP address, billing information, email address, state-issued identification (for identity verification); and "non-personal" data (data that cannot be traced back to an individual, such as anonymized or aggregated information) i.e. information relating to browsing activities, user device, operating system, internet browser, etc.
How is data collected?	Via Individuals directly (when they create an account or contact the App); via third party tracking technologies e.g. cookies, beacons, pixels, tags and scripts (when individuals visit the App or website - the App does not respond to browser "do not track" (DNT) signals); via other third parties (e.g. Apple's Healthkit or Fitbit). To use the App, users have two options: (1) Use the App "anonymously" (choose a username). With this option, users may not recover their information if they uninstall the App or lose their phone. Some services, such as the "Virtual Visit", are also not available; or (2) Create a verified user account (by providing an email address and phone number). When individuals create an account, they may also add information about their medical history, chronic conditions, or smoking habits.
Who can access the data?	"Non-personal" data may be transferred, shared, or disclosed. "Personal" data is "never sold, rented, or shared" with third parties (without explicit consent). It is never shared with advertisers, unless it is non-identifying, non-health information, for the purpose of optimizing internal marketing campaigns. Personal data may also be shared as necessary to protect rights and safety, for mergers & acquisition purposes, and with: K employees and contractors; Third party service providers, which have access according to their purpose, and may only use the information for such purposes.
Purposes the data	"Non-personal" information may be used at the App's sole discretion. Personal data is used for specified purposes: to provide individuals

used for, and purpose limitations	with relevant health information; to improve the Apps AI models; to operate, customize, and improve services; to contact individuals (e.g. for marketing); for other legitimate interests (to enhance data security and fraud prevention capabilities and tools, to support legitimate business interests e.g. identifying user trends, and to comply with laws). Functions and services provided by third parties include: hosting and maintenance, error monitoring, debugging, performance monitoring, billing, customer relationship, database storage and management, and direct marketing campaigns); affiliated doctors for "Virtual Visits"; and law enforcement, legal requests & duties.
Where is data stored?	It may be stored and processed in the US, Israel, or any other country in which the App, or their affiliates, maintain facilities in, and in other jurisdictions as necessary for the proper delivery of services or as may be required by law.
How long is data stored?	All users may exercise the GDPR right to be forgotten to erase personal data. Beyond this, personal data is retained for as long as the user account is active. After an account is deactivated, it may be retained as reasonably necessary to: a) comply with legal obligations; b) resolve user disputes; c) enforce agreements; d) protect legitimate interests.
Monitoring of effectiveness	The more specific the information shared is about an individual's symptoms, the more accurate and relevant information the App is able to provide. Accurate self-reporting relies on trusting users to report consistently. The use of AI to provide individuals with contextual results is effective. A peer-reviewed study of K Health was carried out by Gideon Koran et al (just before the outbreak).
Proportionality, fundamental human rights, and data protection & privacy	Compliant with HIPAA, GDPR, CCPA, and California's Shine the Light law. GDPR rights are granted to all users, regardless of location. When health information is collected when an individual talks to a doctor using the App, it will be subject to HIPAA. The App also participates in the EU-US Privacy Shield Framework and is subject to the powers of the U.S. Federal Trade Commission. The Privacy Policy shall be interpreted in accordance with the laws of the State of New York. The App is only compatible with iOS 12.0 or later for individuals ages 18+. This creates accessibility issues for individuals who do not have access to smartphones, with potential for disparate impact. The App is free of charge and available in approximately 30 languages.
Privacy safeguards	High standards of physical, administrative, and technical safeguards to preserve the integrity and security of all information collected. Third party service providers are also required to maintain the privacy and security of personally identifiable information. The App uses encrypted transportation and storage. Regular system monitoring for vulnerabilities and attacks, and regularly seek new ways and third party services for further enhancing security and privacy. Employee privacy & security training, and internal policies and procedures. Employees are granted minimal access required to perform their duties, and service providers may only access and process data to perform specific functions. When personal data is no longer required for specific purposes disclosed in the privacy policy, it is deleted.
Open source code	N/A
AI/ML claims	K Health uses natural language processing (NLP) and natural language understanding (NLU) to provide a chat-bot interface at the first level of use. The system is described as trained on 2 million anonymized health records from the Maccabi Health Services in Israel but as continuously updated through contemporary patient interaction. In an article published in Medicine (Koren et al 2019), the process is

	described in detail. Standard NLP tools and "proprietary tools" were used to extract features linked to specific conditions from physicians' notes. Training for recognition of symptom patterns included use of structured machine learning to build auto tagging tools to then tag future, unstructured, notes. Using annotated physicians notes, whether the annotation was done by machine or hand, classification and clustering algorithms (e.g., logistic regression models, and random forest classifiers) paired patterns of symptoms and patient characteristics. The associations between symptoms and outcomes were tagged manually then using NLP tools to create new clusters which form the basis of conversational questions that form the basis of conversational patient interaction. Depending on patient answers, they are clustered automatically into cohorts of "Patients Like Me" and given information on conditions others with similar symptoms were diagnosed, medications prescribed, etc. The patient is asked follow up questions at a later date, which are then used to update the system's clusters of information with additional information such as final diagnosis or treatment.

HaMagen (the "Protector App") (Israel)

The App was built by the Government to tackle COVID-19. It intends to alert users of exposure to COVID-19 by comparing movement and location data with that of infected individuals. The data is stored on user devices, and is deleted upon removal of the App from the device. Because the data is stored on user devices, the App states that users shall have no claim for privacy violations as a result of using the App. If transferred to the Ministry of Health with consent, it is not shared beyond employees and service providers. The App acknowledges technical limitations which may possibly reduce accuracy or completeness of data. Privacy Policy: click here. The MOH may change the Terms of Use with notification and consent.

Who built the app?	**Government.** (The State of Israel, through the Ministry of Health).
Intentions and capabilities	The App was built as part of a national effort to tackle COVID-19. The Service does not constitute medical advice, but is intended to alert users to their exposure to Coronavirus patients as soon as possible. The App examines the movement (i.e. the dates, times, and locations) of users in relation to the movement of identified Coronavirus patients according to the information available to the Ministry of Health. Users are provided with alerts if movements overlaps (it is assumed that overlaps in movement mean possible exposure to Coronavirus patients). Users who are diagnosed as Coronavirus patients are also able to retrace their movements in the last 14 days prior to their diagnosis. The intention here is to help notify people whose movements have overlapped with the Corona patient, that they are required to enter home isolation immediately.
What data is collected?	The app collects movement and location information about users.
How is data collected?	Data is collected from the time of installation of the App and not before. "In future versions, it may be possible, with the consent of the user, to receive the location history from Google" (provided that the option to save location history is enabled) from the last 14 days.
Who can access the data?	The data is stored on the user device. However, users who are diagnosed as Corona patients (or their legal guardians) may allow for their information to be transferred to the Ministry of Health (including its employees, representatives and service providers).
Purposes the data used for, and purpose limitations	The movement and location information collected about users is used to create a detailed history of all the places that the user visits and the dates and times of such visits. The information is cross-referenced with the information from diagnosed patients to whom exposure occurred. The information is also used to "help identify exposed people who should enter home isolation immediately." "The Ministry of Health reserves the right to . . . make changes to the App from time to time, and all at its sole discretion.
How long is data	Upon removing the App from a user device, the information stored on the device will be deleted.

stored?	
Where is data stored?	Personal information is stored in the internal memory of the user's cellular device. It is not stored on the servers of the Ministry of Health or any other entity.
Monitoring of effectiveness	There have been over 500,000 downloads. The accuracy of GPS signals vary depending on the weather or physical interference (less accurate in urban areas or inside large buildings e.g., a block of flats). Some of the information is based on data and reports collected by the cellular devices of other users and may contain inaccuracies or be incomplete or erroneous due to technical limitations. Using location data for contact tracing also raises privacy and security concerns. If users are hesitant to download the App for fear of inadvertently revealing their movements, its ability to link the dots would be greatly diminished. The Big Data Institute at Oxford University have concluded that the epidemic can be stopped if contact tracing is sufficiently fast, efficient, and scaled. Effectiveness of contact tracing Apps depends on widespread usage, mobile phone ownership, and widespread testing to diagnose infections in the first place. Because a tracking App cannot capture every possible source of infection, it risks creating a false sense of security for users. It is also likely to be more effective at earlier stages of the outbreak in a specific area to isolate potential cases. However, the World Health Organization and the CDC have advised that social distancing is currently the most effective way to slow the spread of COVID-19. Oxford BDI and SAGE have published information on the efficacy of contact tracing for the containment of COVID-19.
Proportionality, fundamental human rights, and data protection & privacy	The provider claims that collecting the movement and location information is "necessary to provide the services specified and fulfil the goal of the App." People whose movements have overlapped with Corona patients, as identified by this App, will be notified through the App that they are "required to enter home isolation immediately." "[D]ue to the nature of a new App, and under the current emergency circumstances . . . the Ministry of Health cannot guarantee the absolute and continuous availability of the Service without any errors or interruptions." The MOH undertakes to address any such error or interruption, if identified, as soon as possible." However, they bear no responsibility for any direct or indirect damage resulting from any error or interruption in the operation of the App, or for the accuracy of information collected on user devices. As data is only stored on the user's cellular device, users shall have no claim regarding any violation of their privacy as a result of using the App. Imperial College London have released a White Paper outlining eight privacy questions to ask to evaluate COVID-19 contact tracking apps.
Privacy safeguards	The Ministry shall "make every effort" to maintain adequate information security in accordance with the nature of the information collected on the device.
Open source code	Yes. the code has been uploaded to GitHub. This contributes to the improvement of security and transparency and ensures privacy because it enables any security expert or programmer to example the code, and find and fix problematic features.
AI/ML claims	None described.

TraceTogether App (Singapore)

The App was built by the Government to tackle COVID-19 by informing users if they were in prolonged proximity to a person infected. The data is used strictly for contact tracing. It only stores a phone number and a randomized user ID. Location data is not collected. The App uses Bluetooth to approximate users' distance to other phones running the same App, by exchanging a Temporary ID generated by encrypting the User ID with a private key held by the Ministry of Health (MOH). Temporary ID's are regularly refreshed. Privacy Policy: click here.

Who built the app?	**Government.** (Government Digital Services team at Government Technology Agency of Singapore).
Intentions and capabilities	The App "facilitates the contacting process" allowing users to be informed if they were in prolonged physical proximity with an infected person. The BlueTrace Manifesto, outlines the intention to implement the App in an interoperable, decentralized manner.
What data is collected?	The App only stores users' phone number & a random anonymized User ID e.g., [9I8VPeQeWDofj39c8dPySoUXLqh2] generated when a user signs up and associated with the users' mobile number. User location data is **not** collected. Bluetooth is used to approximate users' distance to other phones running the same App. It will identify users who are within 6.5 feet of one another for 30 minutes.
How is data collected?	When a user is close to another phone running the App, both phones use Bluetooth to exchange a Temporary ID. Phones with the App installed send one another a message containing four pieces of information: a timestamp, Bluetooth signal strength, the phone's model, and a temporary identifier or device nickname.
Who can access the data?	The data is never shown to the public. If a user becomes infected with COVID-19, they have the option to give MOH access to their App data. The analysis is done centrally by a trusted public health authority. Sovereignty is respected through a federated model among a network of participating countries and public health authorities.
Purposes the data used for, and purpose limitations	The data will be used solely for contact tracing of persons possibly exposed to COVID-19. Once contact tracing ceases, users will be prompted to disable the Apps functionality. If contact tracking is required for a future outbreak, users will be prompted to enable permissions, or users can reinstall the App.
Where is data stored?	Data about proximate phones is stored only on users' phones. The user data (phone number and username) is stored in a secure server.
How long is data stored?	Records of encounters with other users are stored for 21 days on user devices. If consent is revoked, user data (mobile number and User ID) will be deleted. This "renders meaningless all data that the phone has exchanged with other phones, because the data will no longer

	be associated" with the user. Functionality can also be disabled at any time by turning off the Bluetooth permissions or deleting the App.
Monitoring of effectiveness	Bluetooth may be more effective to determine users' proximite locations than GPS, especially inside large buildings and in urban areas. Bluetooth signal strength varies between phones which makes it difficult to estimate the distance between people. Expert engineers have mitigated this. By not collecting location information, public trust, and therefore downloads and effectiveness, may be heightened. As of March 25, at least 620,000 people had downloaded the App. The Big Data Institute at Oxford University have concluded that the epidemic can be stopped if contact tracing is sufficiently fast, efficient, and scaled. Effectiveness of contact tracing Apps depends on widespread App usage, mobile phone ownership, and widespread testing to diagnose infections in the first place. It is likely to be more effective at earlier stages of the outbreak in a specific area to isolate potential cases. Because a tracking App cannot capture every possible source of infection, it risks creating a false sense of security for users. Nevertheless, the App enables authorities to perform contact tracing more efficiently, especially where infected persons do not know everyone whom they have been in close proximity with. The WHO and the CDC have advised that social distancing is currently the most effective way to slow the spread of COVID-19. Oxford BDI and SAGE have published information on the efficacy of contact tracing for the containment of COVID-19.
Proportionality, fundamental human rights, and data protection & privacy	Consent is required for the App to exchange Bluetooth signals with nearby users. It employs a privacy-preserving method to approximate user location and collects minimal personal information. There are strong guarantees that data will be used strictly for contact tracing. Rather than asking *where* users are, the App asks *who* they came into contact with. If a user is diagnosed with COVID-19, the MOH could be allowed to access the App data to identify people who had close contact with the infected individual. When a person is contacted, they are required by law to assist the health ministry in accurately mapping out their movements and interactions to minimize the risk of widespread infection. The App has been hailed as striking a good balance between the needs of individuals and benefits to society, and there is interest among other Governments in following in Singapore's footsteps. Imperial College London have released a White Paper outlining eight privacy questions to ask to evaluate COVID-19 contact tracking apps. An open letter written by expert technologists praised TraceTogether's clear terms and conditions, and urged others to follow in their footsteps.
Privacy safeguards	The App is "opt in." Consent may be revoked at any time via email with the mobile number used to register in the App. Bluetooth is less privacy-invasive than GPS. The Temp ID generated by Bluetooth to determine users' proximity to one another is generated by encrypting the User ID with a private key held by the Ministry of Health (MOH). It can only be decrypted by MOH and does not reveal user identity or the identity of the other person. Still, the logs can be decrypted and analyzed by the MOH when it is deemed necessary and the users can be easily identified from that information. The Temporary ID is refreshed regularly. The lack of a persistent identifier means it is impossible for third parties to identify or track a user. To preserve privacy, the collection and logging of proximity data between devices is done in a peer-to-peer, decentralized fashion. "While this is an urgent public health emergency, we are committed to safeguarding your privacy and ensuring you have control over your data." 40 engineers spent more than 10,000 man-hours developing the App.
Open source code	The Government plans to open source the App, so that others may implement the BlueTrace protocol.
AI/ML claims	None described.

COVID Symptom Tracker App (UK)

The App was built by a private entity for the purposes of supporting coronavirus research. Currently, it is deployed in the UK. However, the provider intends to release the App in other regions based on an open-source approach. Sensitive personal information (e.g. symptoms) is collected on the basis of individual consent and is processed only for specific research purposes. Third parties have access to sensitive data only for these purposes (with personal details replaced by an anonymous code). Due to the nature of the research purposes, there are no particular time limits on the storage of sensitive personal information. However, it will be kept "no longer than necessary." The App was developed quickly by a small team, and there are currently some accessibility and functionality limitations. The App was released with default permission settings. In practice, it does not use all of those permissions. Recognizing that this is not in-line with best practices, the App intends to remove excessive permissions in the future. Privacy Policy: click here.

Who built the app?	**Private company.** ZOE Global Ltd (a health science company), in partnership with doctors and scientists at King's College London, Guys and St Thomas' Hospital.
Intentions and capabilities	The App was built to support King's College London's vital coronavirus research. It will be used to study the symptoms of COVID-19 and to track the spread of the virus. The research aims to help scientists understand COVID-19, and to eventually help the NHS to support sick individuals. The App creators expect the questions they are asking to evolve as they learn about the virus. The App is currently available in the UK, but the App producers are hoping to release it in other regions soon.
What data is collected?	The App was released with default permission settings. "Sensitive" personal information: health information (e.g. symptoms), device data (e.g. IP address, location). The list of reportable symptoms is reviewed by the latest research and advice from scientists, and additional fields are likely to be added routinely. "Other" personal information (e.g. contact information). Email address is required to register.
How is data collected?	Self-reporting.
Who can access the data?	Third parties process personal data on behalf of the App. "Sensitive" personal information is shared with health researchers i.e. hospital workers, the NHS, universities, health charities, and other research institutions. A full list of the institutions the data is shared with (as of March 30, 2020): King's College London, Guys & St Thomas' Hospitals, NHS, Harvard University, Stanford University, Massachusetts General Hospital, Tufts University, Berkeley University, Nottingham University, University of Trento, Lundt University. A full list of third party processors (as of March 30, 2020): Amazon Web Services, Google Cloud Platform, Survey Money, Segment, Google Analytics, Mixpanel, Google G-Suite, MailChimp, Mailgun, Intercom, Sentry, Google Firebase, SwiftyBeaver. KCL will be "coordinating data sharing with researchers in the UK and other countries to try and learn as fast as possible." "Contact information" is not sold to third-parties.

Purposes the data used for, and purpose limitations	"Sensitive" personal information is never used for commercial purposes. It is solely processed to better understand symptoms of COVID-19, how fast the virus is spreading in specific areas, and to identify high-risk areas in the UK; advance scientific research into the links between patient's health and their response to infection by COVDI19; and to help the NHS to support sick individuals. "Other" personal information is solely processed for developing, marketing, and running the App, i.e., asking for individual feedback on the App or conducting other forms of survey, keeping in touch with individuals about the app and it's performance, and sending information to individuals about new versions of the App or similar Apps that may be provided in the future.
Where is data stored?	In multiple jurisdictions (inside and outside the EU) depending on which institutions and third parties it is shared with.
How long is data stored?	Due to the nature of the research, there are no particular time limits on the storage of "sensitive" personal data. However, it will be kept under regular review to ensure that it is not kept "longer than necessary." To delete sensitive personal information, individuals may withdraw consent to processing via email. "Other" personal information (i.e. contact information) is kept for 6 years after the last communication, or the last use of the App, for liability purposes, after which time it is deleted.
Monitoring of effectiveness	Critics debate the effectiveness and utility of crowdsourced data. Trust is placed in people to be accurate and consistent in how they describe their symptoms. However, the researchers are also using preexisting detailed health information from a cohort of 15,000 twins (e.g. genetic and immune profiling, medical history and lifestyle, and their microbiome). Effectiveness also depends on widespread usage. As of March 27, 2020, almost 2 million people have downloaded the App and the software is scaled to hundreds of millions of users. However, OFCOM figures show that 22% of UK adults do not have a smartphone, rising to 45% of adults over 55. Clinicians and researchers are concerned about vulnerable individuals who may not be able to report symptoms themselves (due to lack of access to the App). Currently, it is difficult to report symptoms on behalf of others (e.g. family members who are elderly or under 18). The App hopes to release functionality in the future to make this easier. There is currently no web based version of the App for those without smartphones. However, the App intends to make this available when they have the resources. The App fails to meet some accessibility standards. For instance, it is not available to those with limited sight. The App provider is working to resolve these issues. The team is "a small, not for profit team" and would "appreciate your patience as we work on [functionality updates]." A number of features may be added in the future, such as: sharing symptoms with others (e.g. family members), or seeing symptoms reported in the local area or across the country. There is a delay between updating the App and Apple and Google releasing updates on the App store. As a result, the functionality to report symptoms (for those who already have COVID-19) is not yet released (as of March 30, 2020). The App was produced in a very short development time, and the App provider has admitted "there may be a bug or two." It welcomes feedback and is working to resolve bugs. For instance, some users have experienced difficulties creating an account.
Proportionality, fundamental human rights, and data protection & privacy	The App was released "quickly with default permission settings" (possibly excessive). The App has recognized that this "fails to meet best practice," because in practice, it does not use all of the permissions. The provider has expressed an intention to remove excessive permissions in the future. On March 23, 2020, a group of leading technologists wrote an open letter to the NHSX and the Secretary of State for Health and Social Care to ensure new technologies and data-driven solutions used in the suppression of Coronavirus follow

	ethical best practices. Reliance of data self-reported from smartphones risks reinforcing existing inequalities, especially if it could be used to establish reasonable or reliable grounds for a person to be detained. In the UK, Part 3 section 61A of the Investigatory Powers Act enables people with symptoms or a diagnosis of COVID-19 to be tracked without notice. The Bill also gives immigration officers and police the power to detain people if they have "reasonable grounds to suspect . . . a person is infectious." Taken together with existing far-reaching data-gather powers creates the risk that location and contact tracking technology could be used as a means of social control. GDPR applies, even to individuals who do not live in Europe. The legal basis for processing "sensitive" personal information is individual consent. The App is not available to under 18's directly, as they must be able to provide consent. The legal basis for processing "other" personal information is their legitimate interest in developing, marketing, and running the App. Sometimes, data is exported to countries such as the USA, which have very different kinds of rules on data protections than GDPR.
Privacy safeguards	When personal data is shared with researchers outside of the NHS or King's College London, an anonymous code is used to replace personal details. Data security is taken "very seriously" and best practices are enforced to ensure personal data is protected. The Privacy Policy outlines individual rights granted under the GDPR, provides contact details to exercise the rights, and points individuals towards more Guidance from the UK Information Commissioner's Office (ICO). When third parties process personal data on behalf of the App, they are prohibited from using it for their own purposes. The App has in place a contract with each processor requiring them to only process the data on the App's instructions and to take proper care in using it. Third parties are not permitted to keep the data after the relationship has ended.
Open source code	The App producers are hoping to release the App in regions outside of the UK soon, based on an open-source approach. The non-profit has called for support from financiers and people skilled in local languages and development skills. Making the code open source would be a positive development. In an open letter written by technologists to the NHSX, expert technologists called upon UK authorities to "institute a culture of working in the open, with clear, regular public communication about projects being undertaken and the publication of machine readable data and models - to build trust and minimise speculation."
AI/ML claims	The machine learning used specifically in COVID-19 Symptom Tracker is not described. This system is built on work by ZoeGlobal, which claims to use gradient boosting regression, ensemble regression models, and random forest forms of machine learning in estimation of physiological responses to food (advanced regression techniques).

Home Quarantine App (Poland)

This App was built by the Government for the purpose of facilitating quarantine compliance of persons suspected of being infected with COVID-19. People may choose between downloading the App or police visits. Users are obliged to periodically upload photos of their faces and to provide their actual and quarantine locations to prove they are at home. Users are required to immediately notify authorities using the App if they develop symptoms. Failure to comply with these obligations results in notification of the authorities and possible legal coercion. Location tracking occurs at all times during the 14-day quarantine. Data is stored for up to 6 years after deactivation of the App. The Privacy Policy is not easily accessible. A download is available in Polish (as of March 30, 2020).

Who built the app?	**Government.** The App was developed by the Polish Ministry of Digital Affairs, in cooperation with the Ministry of Health.
Intentions and capabilities	The App is a preventative element in the fight against the spread of COVID-19. It is designed to make it easier to handle the mandatory 14-day quarantine of citizens (quarantine compliance) who have returned from abroad or who have the virus. It facilitates a basic health assessment, direct notification of any threats, and makes it easier to connect people with social services or request help with urgent supplies.
What data is collected?	Citizen ID (Citizen's technical identifier), full name, telephone number, declared address of stay (quarantine location information), actual GPS location, photo of face (facial recognition), device photos, requested meals, groceries, psychological help and contact.
How is data collected?	Phone numbers are collected on a mandatory basis in order to Register as a verified user. To use the App, users are obliged to take a selfie photo at a declared quarantine facility. Users are randomly prompted to upload more geo-located selfies at regular intervals to prove their whereabouts. To collect location information, GPS location is automatically checked, even when the App is not open. The App requires the device to have enabled access to the internet, camera, location, and photos. The device must have a GPS module and internet access. To receive essential items, users must send a form with requests (e.g. meals, groceries, psychological help or contact).
Who can access the data?	The Government, in particular the Ministry of Health and the Ministry of Digital Affairs; Police Headquarters; Provincial Police Headquarters; voivods; central IT center; Take Task S.A; Center of Health Information Systems.
Purposes the data used for, and purpose limitations	The purpose of the App is to support the services and institutions appointed to help in the event of an epidemic threat (i.e. quarantine compliance). Once the account is deactivated (after 14 days), data will be stored in accordance with certain principles. In particular, user's data are made available to the Services in order to implement their statutory obligations related to comparing the epidemiological threat caused by COVID-19. The data is not processed for purposes of marketing.
Where is data stored?	Government servers (not on the device). User's data are made available to the Services in order to implement their statutory obligations

	related to comparing the epidemiological threat caused by COVID-19.
How long is data stored?	The Minister stores personal data for the limitation period for claims referred to in Article 118 of the Act (see below) (6 years), which will be counted from the moment of deactivation of the App.
Monitoring of effectiveness	The WHO and the CDC have advised that social distancing is currently the most effective way to slow the spread of COVID-19. However, some users have reported bugs and redundant police visits. Many users have said that the App was prone to failure (e.g., digital service freezing when individuals try to upload photos, failure to store images in the Government database, and App selfie requests being made even after the police give the all clear). The Polish Government created it in three days based on an out-of-the-box service offered by a third-party developer. The User bears full responsibility for violation of law or damage caused by the User's actions related to their use of the App (in particular the accuracy of the data provided and installing security updates). The App has been downloaded by more than 90,000 people, according to government figures (as of April 2, 2020). Questions have been raised about how the elderly and others with limited access to smartphones could participate. A Government spokesperson has said that exemptions would be made for those who did not have internet access or who do not own a smartphone.
Proportionality, fundamental human rights, and data protection & privacy	Quarantined citizens are given the choice of police visits or downloading the App. The Polish Government is reportedly automatically making accounts for suspected quarantine patients. The App assists authorities to enforce the quarantine of users infected with COVID-19. It is designed to monitor the implementation of quarantined people suspected of carrying COVID-19 using location data and facial recognition. In case of COVID-19 symptoms, users are obliged to immediately notify the relevant departments using the App. Users will be prompted to upload photos at unexpected times throughout the day. If users do not upload selfies within 20 minutes (or when other obligations are violated) the authorities are notified, which may result in coercive application of the law (e.g. monetary fines) if quarantine is violated. Quarantined individuals are subject to obligations imposed on them by the Journal of Laws of 2019, item 1239 (aka "Dz. U. z 2019, poz. 1239 z późn. zm") - a law to prevent and combat infections and infectious diseases. The App is compatible with iPhone (iOS 10.3 or later or Android 6.0 or higher). The device must have a GPS module, internet access, a camera with a minimum resolution of 5Mpix and the ability to record video. It is only available for people aged 18+.
Privacy safeguards	The App is technically opt-in. The administrator has appointed a Data Protection Officer who can be contacted in matters relating to personal data processing. GDPR applies. This processing takes place due to an important public interest (i.e. a crisis situation related to the spread of COVID-19) - Article 9, paragraph 2 of the GDPR.
Open source code	N/A
AI/ML claims	No facial recognition. This system uses the innate facial detection and image classification features of a users' phone. Selfies are taken by the person using the app, thus the detection and classification features any user interacts with varies by operating systems and other software, and cameras and other hardware, on the users phone.

Decentralized Privacy-Preserving Proximity Tracing (DP-3T) (EU)

DP-3T is an international initiative providing technical standards, mechanisms, and services creating interoperability to local implementations. The mission of DP-3T is to assist national initiatives by supplying a set of ready-to-use, well-tested and properly assessed mechanisms and standards, as well as support services for interoperability, outreach and operation if needed. These fully protect privacy and leverage the possibilities and features of digital technology to maximize speech and real-time capability of any national pandemic response. These mechanisms include well-tested proximity tracking technologies, secure data anonymization, trustworthy mechanisms to enable contact between user and health-officials in a data protection conforming environment, APIs that can provide anonymized contact chains as well as risk-scoring to other applications (e.g. for health resource management, private risk management, or other pandemic response systems). They aim to provide building blocks (under an open source licence) for creating local Corona-finder-Applications as well as secure and scalable backend services that can deal with hundreds of millions of registered devices per country.

Who built the app?	**Pan-European researchers** (130 academics, activists, and technologists). Eight countries have taken part in the project so far (Austria, Belgium, Denmark, France, Germany, Italy, Switzerland, and Spain). So far the PEPP-PT team includes scientists, technologists and experts from well-known international institutions and expert companies who can cover the areas of communication, psychology, epidemiology, proximity-tracking, security, encryption, data protection, application development, scalable systems, supercomputing infrastructure and artificial intelligence.
Intentions and capabilities	The mission of PEPP-PT is to assist national initiatives by supplying a set of ready-to-use, well-tested and properly assessed mechanisms and standards, as well as support services for interoperability, outreach and operation if needed. The effort aims to use mobile phones to contain the spread of COVID-19 by publicly releasing software for an internationally applicable proximity tracing mechanism which interrupts new chains of COVID-19 transmissions and alerts users who have been in close proximity with infected persons in the preceding days (even if the chain was started abroad). The aim of releasing the code is to facilitate the launch of national Apps across the region (and outside of the EU) that can communicate with each other to pick up Bluetooth signals and help avoid infections. Since a long-term lockdown to slow the spread of the virus is not economically viable, the effort aims to tackle the urgent question of how to open society and maintain the economy without risking a collapse of the healthcare system. By creating interoperable software for an App, the technology will facilitate the resumption of international business and personal travel. The idea is to make the technology available to as many countries, managers of infectious disease responses, and developers as quickly and easily as possible.
What data is collected?	The anonymous ID of each user who is in epidemiologically sufficient proximity to a user infected with COVID-19 for an epidemiologically sufficient period of time (approx 2 meters for 30 minutes). Only the proximity history that could be relevant for the virus is saved. No

	geolocation, no personal information or other data are logged that would allow the identification of the user. There is no transmission by which person, where or when an infection could have taken place. This makes the European App idea more privacy-friendly than the TraceTogether App, which stores the phone numbers of users.
How is data collected?	Two phones never exchange data directly. Each PEPP-PT phone broadcasts over a short distance a temporary valid, authenticated and anonymous identifier (ID) that cannot be connected to a user. Proximity between phones of other PEPP-PT users are estimated by measuring radio signals (Bluetooth, etc) using well tested and calibrated algorithms.
Who can access the data?	If a user has not been tested or has tested negative, the anonymous proximity history cannot be viewed by anyone, not even the user of phone A. It is not accessible by third parties (Government or private entities). If a user has been confirmed to be COVID-19 positive, the health authorities will contact the user and provide a TAN code to them to use to voluntarily provide information to the national trust service that permits the notification of PEPP-PT Apps recorded in the device proximity history and hence potentially infected. Since the history contains anonymous identifiers, neither person can be aware of the other's identity. Rather, a user may poll the server to verify whether their ID is in the dataset provided by the infected user(s). The anonymous IDs contain encrypted mechanisms to identify the country of each user. Using this information, anonymous IDs are handled in a country-specific manner.
Purposes the data used for, and purpose limitations	Analysis of Bluetooth signals between mobile phones to detect users in close proximity. Used for contact tracing to alert users in close enough proximity to infected users to create an exposure risk. If a user becomes infected, the App alerts others who have been around them in the preceding days.
Where is data stored?	The anonymous ID of phone B is recorded in the encrypted proximity history stored locally on phone A (and vice versa).
How long is data stored?	Temporarily. Older events in the proximity history are deleted when they become epidemiologically unimportant.
Monitoring of effectiveness	To be effective, a large proportion of the population must download the App. Downloads by approx 40- 60% of the population would be "ideal." However, in principle, even a few people using the App would "make a difference." Each country must convince its citizens to participate in such a system. A recent OSF study found that around 75% of the German population would download a Corona tracing app, with similar results in the UK, France, and Italy. However, the problem remains that especially the more vulnerable older citizens often do not have a smartphone or do not always have it with them. The App is scalable and open, and can be used by any country. The backend services are secure and scalable - they can be deployed into local IT infrastructure and can deal with hundreds of millions of registered devices per country. PEPP-PT can also provide support in implementing and financing local "installation" and "trust" campaigns. The aim of releasing the code is to facilitate the launch of interoperable national Apps across the region that communicate with each other & help avoid infections more effectively. Pan-European cooperation and collaboration also bundles expertise in an efficient and targeted manner. A process for how to inform and manage exposed contacts can be defined on a country-by-country basis. By providing a TAN code to users who have tested positive for COVID-19 for the purposes of providing the data, it is ensured that

	potential malware cannot inject incorrect information into the PEPP-PT system. Unintended effects are guarded against by encouraging national security agencies and national data protection agencies to inspect the code and procedures regularly for loopholes. The effort will only be effective in combination with other measures, such as widespread testing and isolation of confirmed cases and their contacts. Isolation of contacts is necessary and effective to prevent further transmissions. The challenge in the current situation is the speed with which the virus spreads, as well as the already high case numbers. Oxford BDI and SAGE have published information on the efficacy of contact tracing for the containment of COVID-19.
Proportionality, fundamental human rights, and data protection & privacy	The underlying technology is developed in a constant exchange with data protection experts and ethicists. This somewhat aligns with calls by technologists to the NHSX in a recent open letter for the introduction of "bold emergency governance measures, including privacy and rights impact assessments and the drafting of an expert governance panel . . to ensure innovation works and is held to account." Striking the appropriate balance between public health and safety while maintaining high standards of privacy is central to the PEPP-PT project. A central principle driving the work forward is to "not allow a health crisis to lead to a weakening of privacy that so many generations before us have fought for." By making the code widely available and using Bluetooth signals, effectiveness may be relatively high. Meanwhile, privacy is preserved. So far, infection tracking has largely been done by interviewing those who are infected. However, this is inefficient and prone to errors, with patients often unable to remember everyone they crossed paths with in the preceding two weeks. The technology was explicitly created to adhere to strong European privacy and data protection laws and principles. PEPP-PT enables these national initiatives to focus on integration into national processes, national law, customs, and requirements. PEPP-PT offers a certification service for local initiatives so national authorities can release applications with a high level of trust, built on both their credibility and the certainty that European standards in data protection, privacy and security are enforced at all time, and that cross-border interoperability is supported. The initiative is financed through donations and has adopted the WHO standards for such financing to avoid external influence. Imperial College London have released a White Paper outlining eight privacy questions to ask to evaluate COVID-19 contact tracking apps.
Privacy safeguards	The App is opt-in. Even if a user tests COVID-19 positive, they may only share their health status voluntarily with other users who have been in their proximity. Since the proximity history contains anonymous identifiers, neither person can be aware of the other's identity. The code embeds safeguards to encrypt data and anonymize personal information, making it virtually impossible to reveal the identity of the people using the devices. As well as never exchanging data between phones directly, users' aliases are changed frequently. (By not exchanging data directly between phones when users are proximate to one another, this differentiates it from the TraceTogether App). All procedures, mechanisms, standards and code is continuously monitored by the PEPP-PT security team. In parallel, national cyber security agencies and national data protection agencies inspect all of the code line-by-line on a regular basis and sign. Based on the mechanism, each country can develop their own app and provide their own secure infrastructure.
Open source code	Yes.
AI/ML claims	None explicitly described. Claim to have input from artificial intelligence experts. Algorithms are used to measure user proximity between users with radio signals (e.g. Bluetooth).

** Post the date of this chart, the PEPP-PT and DP3T efforts splintered and took very different directions.*
** This chart does not seek to assess data protection risks, but rather describes the data practices of the app on April 3, 2020.*

By Pollyanna Sanderson, Policy Counsel at Future of Privacy Forum. Did we miss anything? Let us know at psanderson@fpf.org.