The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing apps – and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues applicable to contact tracing across a range of key jurisdictions in real time.

Is technology being used by the government to monitor and control the spread of COVID-19 (e.g. contact tracing app, CCTV, cell phone location data, credit-card history)?

In the U.S., there has been some minimal, state-level efforts in this area, but the main effort has been through a major collaboration between Apple and Google. The tech giants are releasing an API in mid-May that can be used in official public health apps in the iOS and Google Play stores. Although these apps have not been rolled-out yet, they are imminent. The API uses detection of Bluetooth signals in order to track location of users over time. If User A has been in close contact with User B, who later self-identifies as having COVID-19 within a pre-defined time window, then User A will be alerted of the potential exposure.

What are considered to be the major privacy concerns in relation to the app in your jurisdiction (in relation to its use (a) by the government; and (b) by private sector organisations)?

The major privacy concerns that would normally be associated with this type of data collection appears, on paper, to have largely been mitigated through the use of a complex public key cryptography infrastructure developed by Apple and Google for this API. The devil of course, is always in the detail, and so we will be able to better judge when apps using this API go live. At this point, notwithstanding a fair amount of noise in the media about privacy concerns, this approach could work well, if the crypto implementation by Apple and Google is sound.
Contacts

Chris Cwalina  
Global Co-Head of Data Protection, Privacy and Cybersecurity  
Washington DC  
Tel +1 202 662 4691  
chris.cwalina@nortonrosefulbright.com

Steven Roosa  
Head of NRF Digital Analytics and Technology Assessment Platform, United States  
New York  
Tel +1 212 318 3222  
steven.roosa@nortonrosefulbright.com

Marcus Evans  
Head of Data Protection, Privacy and Cybersecurity, Europe  
London  
Tel +44 20 7444 3959  
marcus.evans@nortonrosefulbright.com

Ffion Flockhart  
Global Co-Head of Data Protection, Privacy and Cybersecurity  
London  
Tel +44 20 7444 2545  
ffion.flockhart@nortonrosefulbright.com

Anna Gamvros  
Head of Data Protection, Privacy and Cybersecurity, Asia  
Hong Kong SAR  
Tel +852 3405 2428  
anna.gamvros@nortonrosefulbright.com

David Kessler  
Head of Data and Information Risk, United States  
New York  
Tel +1 212 318 3382  
david.kessler@nortonrosefulbright.com