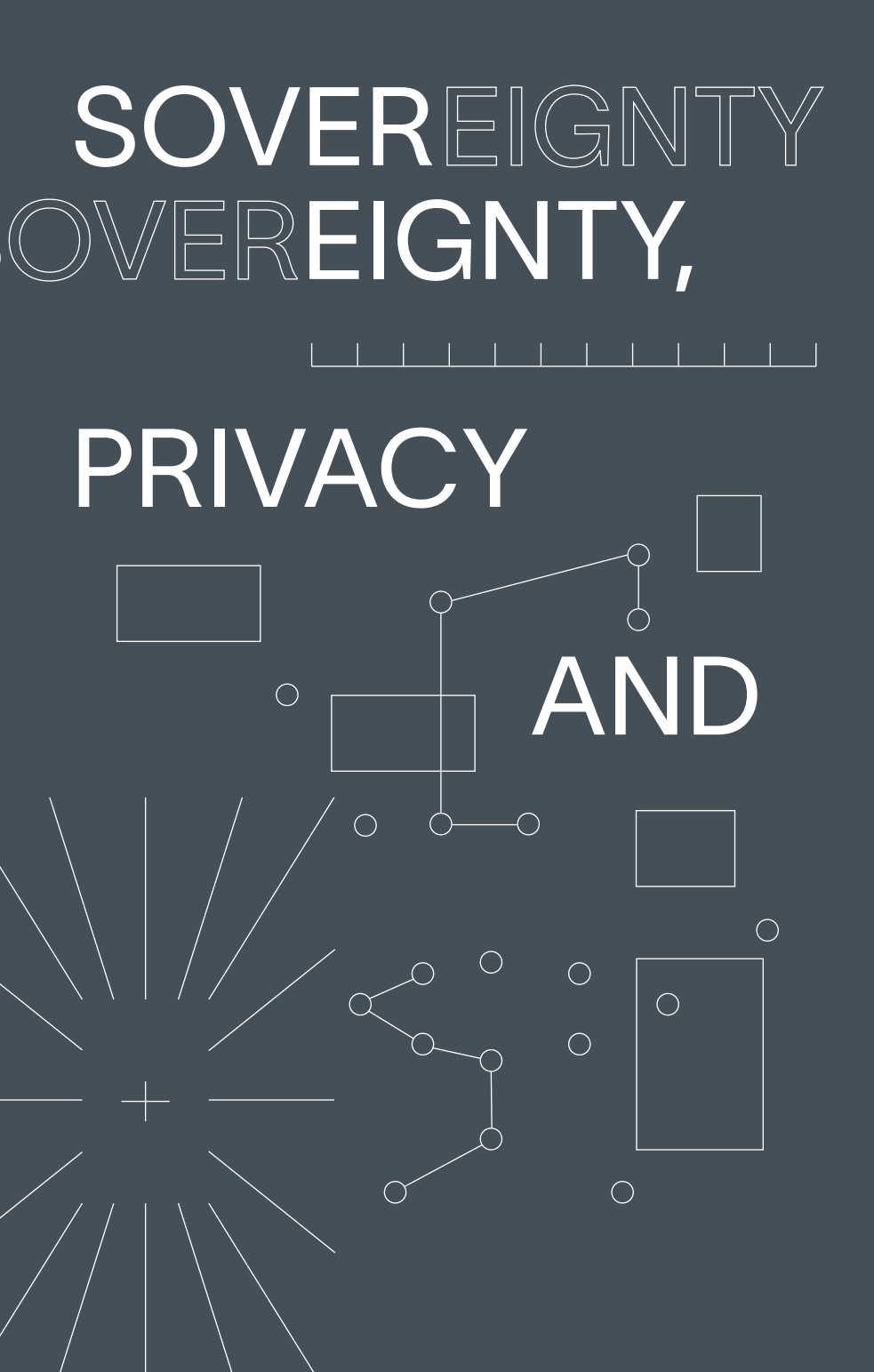
SOVEREIGNTY
SOVEREIGNTY,
PRIVACY
AND



CONTACT TRACING

PROTOCOL PROTOCOLS

Michael Veale

Bluetooth-based COVID-19 contact-tracing apps became an international meme in early 2020. As the crisis headed from epidemic to pandemic, I joined an international consortium of researchers who were concerned about the potential for misuse, mission creep, and abuse of these new infrastructures. Our intervention was to create a decentralised open protocol and codebase called Decentralised Privacy-Preserving Proximity Tracing (DP-3T). It used cryptographic methods to enable smartphone owners to be notified if they had a significant contact event (insofar as Bluetooth can detect it) with a later diagnosed individual, but without requiring a centralised database or persistent identifiers. In contrast, centralised systems, such as Singapore's early *TraceTogether* app, effectively broadcast an ID card that only the state can read, centralising a social graph of physical interaction by requiring diagnosed individuals to upload

data about other people's co-location. DP-3T removed this centralised database to limit data repurposing beyond public health, and removed persistent identifiers to limit function creep towards quarantine control or 'immunity certificates.'

The DP-3T project, then featuring eight universities, was initially part of a pan-European consortium set up in response to COVID-19 called Pan European Privacy-Preserving Proximity Tracing (PEPP-PT), which intended to develop privacy-preserving contact tracing as a partnership between academia and industry. Over time we became increasingly frustrated with PEPP-PT's industrial leadership pushing centralised approaches to governments behind closed doors, using our team's academic credibility to do so, which concerned us. We published the DP-3T protocol in early April for discussion and feedback, but it soon became apparent that PEPP-PT was building a Trojan horse: using the privacy community's wide approval of our public system to slip their own, unpublished centralised approach into deployment. DP-3T universities resigned from PEPP-PT, and despite hiring several crisis PR firms in response (including the German firm notable for its work for Volkswagen in *Dieselgate*), the consortium eventually collapsed.

In parallel, the tech giants entered the scene.

All state-sponsored COVID-19 apps are de facto public–private partnerships between a government, Apple, and Google. Effective enclosure has meant software can only run on the firms' devices with their blessing. Papal levels of blessing are required if unusual sensor access is desired, and the Bluetooth access needed for contact tracing is unusual. Apple typically restricts the use of Bluetooth when apps are off-screen ('backgrounded') through a mixture of software and App Store 'soft law' in order to limit covert, commercial tracking. Apps based on Singapore's *TraceTogether* required problematic technical workarounds. iPhone users had to leave the app open, phone screen on, and unlocked in their pockets as they went about their daily business. This was an inconvenient, insecure, and damaging requirement, crippling participation rates.

In a surprising partnership, Apple and Google announced a system that became known as Exposure Notification on April 10, 2020. This system allowed apps made by national public health authorities to use Bluetooth in the background, although with conditions. Background Bluetooth use was conditional on use of the new Exposure Notification API (instead of the regular code needed to call Bluetooth from apps). This code, explicitly stated by the firms as based on DP-3T, was buried at the operating system level. Importantly, it was deliberately missing a building block that centralised systems would need: it did not allow the app to obtain a list of all identifiers the phone has seen. Centralised apps need these, as they rely on diagnosed people uploading the identifiers of others they have been close to. Decentralised apps, however, only ever transmit information upon diagnosis that an individual's device emitted; the identifiers relating to others that a device heard never need to leave it. This was a conscious move: the firms—or at least Apple, whose operating system was the main impediment to Bluetooth use—would not permit centralisation of data.

A PR-friendly narrative for the firms' actions would state that, pressured around the world and with time constraints to match, they had to engineer a system for a country with minimal legal privacy protections in mind. The European Parliament had indeed demanded decentralisation in a resolution on April 17, 2020, and the European Data Protection Board had also expressed this preference. Building these restrictions into code, rather than the 'soft law' of what can be accepted into the App or Play Stores, would bind their own hands more successfully against government pressure, as a secure operating system update relating to increasing functionality of core sensors is not a quick task.

The consequences of this decision go beyond that, however. Centralised and decentralised proximity tracing systems are largely incompatible. To open up Europe's closed borders, interoperability became high on the agenda. A mass of centralised systems creates coercive pressure for centralisation, and vice versa. Before long, Germany, Switzerland, Estonia, Italy, and many more countries had designed and/or deployed systems based on DP-3T,

Exposure Notification, or both. At the time of writing in June 2020, interoperability was in an advanced state of discussion. Removing friction within a walled garden rather than with outside it, is, of course, straight out of the classic platform playbook.

Some states, notably France, were furious at Apple's decision, declaring it to be an attack on their sovereignty. France wanted a centralised system, stating a desire to mitigate a particular niche snooping attack possible for a tech-savvy neighbour, which affects all Bluetooth contact tracing systems to some degree. NHSX, the tech branch of NHS England, wanted centralisation to experiment with fraud detection, given that a lack of speedy tests in the country meant they wished for an app to allow for abuse-prone self-reporting rather than only test-based diagnosis. Oddly, it is notable that there has been little appetite to attempt to rectify this situation with the legal obligations that sovereign states have at their disposal; instead reifying the view of tech giants as state-like themselves, diplomatic interlocutors rather than firms operating under national law. Sovereignty was mourned before any of its traditional tools were even reached for. Privacy researchers by and large cautiously welcomed the Apple–Google partnership as it provided assurances over short-term COVID-19 surveillance and centralised data breach concerns, but were rightly wary of the obviously unchecked—and potentially uncheckable—power of these platforms.

This ongoing saga highlights the need to think of new ways to control platform power in years to come. While in DP-3T we built a tool that preserved confidentiality, this does not mean it doesn't wield power, or that it sidesteps issues of justice. Google, for example, has been experimenting with federated learning in the Chrome browser—where separate personalisation or targeting algorithms are built for each person without much or any data leaving an individual's device—and has toyed with abolishing third-party cookies. This would preserve confidentiality, but continue to allow firms to optimise, intermediate between, and manipulate populations very similarly to the ways they do currently. Individuals, communities, and governments have limited

power to control the code that runs on their devices, and by extension the protocols they participate in, while the designers of privacy-preserving technologies typically (and strangely) build systems with the assumption that they retain the right to refuse software. To change the status quo of global systems governed by global firms is to open Pandora's box. Both the chance for individuals to escape platform power, but also the chance for states to demand changes such as the abolition of end-to-end encryption, might lurk inside. The drama of contact tracing applications has laid bare how much of both extractive *and* protective infrastructure is reliant on the choices of a small number of gargantuan corporations. A surprising legacy of COVID-19 might be the new visibility of these protocol politics to politicians, who may yet decide to shake up the situation in the years to come, with consequences that remain hard to anticipate.

Michael Veale is lecturer in digital rights and regulation at University College London. He is a co-author of the decentralised Bluetooth proximity tracing protocol, DP-3T.