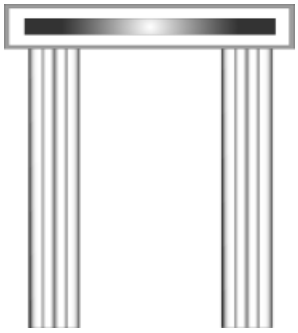
Anthony Speaight QC

Covid-19 Contact Tracing

How Should Policy Proceed?

POLITEIA



POLITEIA

A Forum for Social and Economic Thinking

Politeia commissions and publishes discussions by specialists about social and economic ideas and policies. It aims to encourage public discussion on the relationship between the state and the people. Its aim is not to influence people to support any given political party, candidates for election, or position in a referendum, but to inform public discussion of policy.

The forum is independently funded, and the publications do not express a corporate opinion, but the views of their individual authors.

www.politeia.co.uk

Covid-19 Contact Tracing
How Should Policy Proceed?

Anthony Speaight QC

POLITEIA

2020

First published in 2020
by
Politeia
14a Eccleston Street
London
SW1W 9LT
Tel: 0207 799 5034

E-mail: secretary@politeia.co.uk
Website: www.politeia.co.uk

Cover design by John Marenbon

THE AUTHOR

Anthony Speaight QC is a barrister at 4Pump Court. He was a member of the Government Commission on a UK Bill of Rights. He recently co-authored *Pardonable in the Heat of Crisis – but we must urgently return to the Rule of Law,* with Guy Sandhurst QC. He is past Vice-Chairman of the Bar Council's IT panel. Currently he is Chair of Research of the Society of Conservative Lawyers, but writes here in a personal capacity.

Table of Contents

Introduction

Contact Tracing and Government Policy

The government intends that contract tracing will play an important part in the UK's safe return to work. But the question it must now consider is how best can this laudable aim can be achieved? There are signs that ministers may be weighing up whether to persist with the trials of the unproven app proposed by officials. Not only has the app prompted concerns about a bureaucratic apparatus with the potential for unprecedented intrusion. But the loss of public trust that would result were the app to fail could diminish the very take-up on which the success of a tracing programme depends. Should the government therefore pause before rushing ahead with this app, and consider other systems to achieve its aims?

The value of tracing the contacts of individuals infected with Codid-19, so far as it can be achieved, is widely recognised. There is also wide acceptance that, faced with the gravity of the current emergency, it is worthwhile to attempt to trace infectious contacts through a smartphone app, although there is as yet no certainty how much this will achieve. The issue is as to the choice which has been made between two significantly different types of app, and the lack of safeguards being offered with the method which has been chosen.

It is impossible to understand why the seemingly technical question of the choice between two systems raises fundamental rights issues without some explanation of the two options.

.

I

which App? Decentralised or Centralised?

The Decentralised Model

One option is often referred to as the decentralised system. The first version of a decentralised system was developed by a group of academics including the British academic, Dr Michael Veale of University College London. The arrangement is called Decentralised Privacy-Preserving Proximity Tracing or "DP3T". Its name indicates its purpose – to achieve tracing without comprising personal privacy in respect of a matter as sensitive as coronavirus infection. A similar scheme has been developed by Apple and Google working in conjunction and has reached a stage of development for the companies to be able to make it available.

The decentralised schemes are ingenious. They rely on the software installed on a user's mobile telephone constantly emitting signals through the Bluetooth technology. The decision to install the app is voluntary. The app may be deleted from the phone by the user at any time. The signals in question, which are variously referred by technical experts as "identifiers" or "tokens" or "keys", consist of a long list of seemingly random and meaningless numbers. Other smartphones pick up and temporarily store these signals.

For ease of describing how the arrangement works, let us imagine two individuals, A and B, both of whom have installed the app on their smartphones. A and B, who are not part of the same household, meet each other in a park and sit talking on a bench. Later A tests positive for Covid-19. A may then notify a central server. There is no compulsion on A to do so, although clearly it is a public spirited action and one which the user probably had in mind when deciding to instal the app. The notification involves disclosure of only the identifiers which the phone has emitted over the recent past, probably the previous 14 days. Meanwhile the phones of other users are at regular intervals downloading from the central server the list of identifiers which have been notified by individuals diagnosed with Covid-19. Thus the phone of B spots a match between an identifier on the infected list and an identifier stored in B's phone. The app on B's phone then generates a warning to B.

The Apple/Google scheme involves encrypted data. No governmental or public health authority receives any notification. The central server acts solely as a communication platform. The match between identifiers is made on B's phone. The fact that B has been notified of the contact is wholly and completely private to B. B may, of course, seek advice from a health authority, but doing so is B's choice. No location data relating to the meeting between A and B is stored anywhere.

The Apple/Google initiative has several valuable technical features. It is interoperable between the different types of smartphone. The Bluetooth signals are emitted even if the phone is locked. The operation is low energy, so that it ought not to drain a phone's battery.

The Centralised Model

The British Government has launched a different scheme, which the residents of the Isle of Wight are currently being urged to instal on their phones. This system has been developed by a technology unit with the curiously anonymising of NHSX. NHSX is described as a unit bringing together teams from the Department of Health and Social Care, NHS England and NHS Improvement.

NHSX's scheme is of the type known as centralised. It, too, involves an app using the Bluetooth technology. But unlike the decentralised schemes, there is a central pool of information on a server operated by the public health authority. Whereas under the Apple/Google scheme the identifier signals on A's phone are randomly generated on A's phone, under the NHSX scheme a central server provides identifier signals for A to transmit. B's phone, on picking up identifiers, reports to the central server. It is the central server which spots matches in the event of A reporting an infection. Thus the central server has information about both persons who are infected and persons who has been in proximity to them.

Concerns about the NHSX system exist for three broad reasons. The first is the potential, once such a centralised system is up and running, for it to be developed into a wider apparatus of national surveillance. The second is significant uncertainty as to its compliance with data protection law. Thirdly, there are practical shortcomings, including its insecurity and lack of capacity to work with the systems in other countries.

The first concern: the potential for mission creep to national surveillance

The most fundamental concern is the potential which is created for a "mission creep" to a system of public health surveillance. The issue here is the potential for the future, not the present actuality of what is happening in respect of the Isle of Wight. Currently the NHSX scheme involves the central pool of information containing little more than the fact of the contact between A and B. But there are indications that NHSX is interested in expanding the amount of information which it will obtain. Indeed, the very reason for its preference for a centralised system over a decentralised system is this very possibility of increasing the information obtained.

Giving evidence to the Parliamentary Joint Committee on Human Rights on 4th May 2020 Mr Matthew Gould, the chief executive officer of NHSX[1], said:-

> "[I]f privacy were the only thing that we were optimising for, a decentralised approach could well be the default choice. But, actually, we are balancing a number of things. We are balancing privacy with the need for the public health authorities to get insight into what symptoms subsequently lead to people testing positive, for example, which kinds of contact are riskier, and what changes occur in the nature of contact between, say, three days and one day before symptoms develop."

So the first point to notice is that the explicit justification for the choice of the centralised system is its capacity to acquire more information. That is not in itself a criticism: the acquisition of information about how the virus spreads is plainly in itself a public good, and one which NHS epidemiologists are properly keen to maximise. The issue is the potential for the system, once in place, to be extended.

That some expansion of the information collected is envisaged by NHSX is frankly admitted. In a blog post Mr Gould has written,

> "In future releases of the app, people will be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends."

Mr Gould told the Parliamentary Committee:-

> "If you have a centralised approach, it becomes more straightforward to hone your understanding and decision-making inside the app, which will allow you, for example, to make

[1] Oral evidence at https://committees.parliament.uk/oralevidence/334/html/

> sure that symptoms become more accurate over time and you get a better understanding of when the most dangerous time in somebody's development of symptoms is for them to be having proximity events. Over time, it will tell us whether, for example, five minutes at one metre away is rather more important than 15 minutes at two metres away."

So NHSX hope to collect information not just on the date of A's meeting with B, but also on how long their conversation lasted and even how close they sat on the park bench.

Again, the possession of such information by researchers may not in itself be a bad thing. The point at this stage is simply to observe that NHSX hope in future to expand the information which they collect through the app. The concern is how far the mission creep might go.

At present NHSX heavily stress that the installation of the app and its use are voluntary. But suspicions lurk that some elements in authority may envisage linking the removal of some lockdown restrictions with use of the app. Mr Alex Wickham, the Political Editor of Buzzfeed, claiming sources for his piece, wrote on 18th April[2],

> "Officials are looking at how to enforce use of the app, potentially even requiring people by law to have it on their phones if they want any lifting of lockdown restrictions to apply to them."

It must be recalled that some citizens cannot afford to acquire a smartphone, and some people, especially the elderly, have difficulty in knowing how to download or use an app. The imposition of sanctions on individuals for non-use is not confined to the adoption of a policy to do so by central government. It could well happen in the private sector: an employer might require its workers to use the app, or a shop might admit only customers who carried a phone with an app installed.

These fears could be dispelled if the Government were to accept a well developed proposal for legislation embodying safeguards. Professor Lilian Edwards of Newcastle University, leading a team of academics from eight universities, has published a draft Coronavirus (Safeguards) Bill. This Bill would prohibit sanctions of any kind for failing to carry a phone on which the app had been installed. To date there has been no sign of willingness on the part of the Department of Health to accept such legislation. There has been no White Paper, and no parliamentary debate. In the absence of the enactment of such safeguards to instal the app the question inevitably remains, "If you do not intend detriments on nonusers of the app, why will you not accept this Bill?"

Concerns about how the NHSX app could be used are not assisted by the requirement, despite the protestations that locality is not being traced, for users to supply the first part of their postcode. The justification offered is the NHS desire to track where there may be demand for hospital facilities. Yet the NHS already has an abundance of information on this, as manifested by the publication of data on the incidence of infection by districts. It is hard not to sense the natural inclination of public sector administrators to hoover up as much data as they can.

The second concern: clash with data protection law

The second problem with the NHSX scheme is that it is susceptible to court challenges under data protection law. As is well known, the UK participated in the enactment of the EU's General Data Protection Regulation, and has decided to retain the GDPR in domesticated form. Since 31st January 2020, when the UK exited the EU, the GDPR in its EU form is effective by virtue of the EU (Withdrawal

[2] https://www.buzzfeed.com/alexwickham/coronavirus-uk-lockdown-three-stage-exit-plan accessed on 13th May 2020

Agreement) Act 2020[3]. After the end of the implementation period, which by law is currently 31st December 2020, provisions, which in substance are identical, will be operative under what is known as GDPR UK.

Despite some protestations from the NHSX to the contrary, it seems likely that a court would consider that the NHSX scheme involves the processing of "personal data". "Personal data" means information relating to an identified or identifiable living individual[4]. Most commonly identification is by the individual's name, but it can be in other ways. This includes data which, in the data protection jargon, "individuates" a person. In *Vidal-Hall v Google* in 2016 the Court of Appeal was concerned with the information about websites visited by a computer browser, which is known as browser generated information or BGI. The judgment of Lord Dyson, Master of the Rolls, stated[5],

> "Identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user."

Since the very function of the central server in the NHSX's app is to differentiate A from every other user of the app, it individuates A. That remains so, despite A's identity being pseudonymous. Furthermore, the system enables NHSX to build up a picture of everybody with whom A has been in contact, from which identification could occur.

By contrast, it seems likely that a court would hold that the Apple/Google scheme does not involve the processing of personal data: that, at any rate, is the opinion of the Information Commissioner[6]. From these characteristics of, on the one hand, centralised and, on the other, decentralised schemes flow significant legal advantages of decentralised schemes.

A central plank of data protection law is the prohibition on the processing of personal data outside defined situations. In simple terms, there are two main gateways to permissible processing: one is consent, the other necessity for a public interest. The NHSX scheme faces difficulties in passing through either gateway.

---

[3] The 2020 Act inserted a new s.1A(2) into the EU Withdrawal Act 2018 stating: "The European Communities Act 1972 as it has effect in domestic law ... immediately before exit day, continues to have effect in domestic law ..."

[4] Definition in Data Protection Act 2018, summarising definition in GDPR Art 4(1).

[5] [2016] QB 1003 at [115]

[6] Information Commissioner's Opinion dated 17th April 2020 on "Apple and Google Joint Initiative on COVID-19 Contact Tracing Technology"

II

Processing Personal Data

Legal Boundaries & Practical Arrangements

Consent - The difficulty in passing the consent gateway

In practise, the consent of the data subject is by far the most common basis for processing personal data – as we are all made so aware by the frequency with which we are irritated by computer requests to consent to this or that. NHSX will doubtless argue that consent exists since installing the app is voluntary, and since uploading a notification of infection is also voluntary. But there are several problems with that argument. To be valid, consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes"[7]. It is hard to demonstrate the giving of consent to a public authority owing to the imbalance of power between such an authority and an ordinary citizen[8].

Next consent must be given not just at large but for the specific purpose in question: a data subject may consent to a controller processing for one purpose but not to processing for a distinct purpose[9]. Thus consent given to processing by the NHSX central server for the purpose of contact tracing may not extend to the purpose of the NHSX building up a broader profile of the population for research purposes.

Finally, it is a facet of valid consent that it may be withdrawn at any time, and that "it shall be as easy to withdraw as to give consent"[10]. Mr Gould admitted to the Joint Parliamentary Committee that once a user had uploaded information on his or her infection, it would not be possible to accede to a request from the user to cease processing of that data:-

> "Q: Once someone's data has been sent to the centralised collection area, can that person request that their data is deleted?
>
> Matthew Gould: No. The data can be deleted as long it is on your own device. Once it is uploaded, it becomes enmeshed in wider data, and the technical difficulties of deleting it at that point become tricky."

Public Interest: The difficulty in passing the public interest gateway

If, then, the consent gateway is dubious, what about a public interest argument? Data relating to health faces a stiffer test than less sensitive information about an individual. The most promising routes would appear to be those set out in GDPR art 9 as for the public interest in the area of public health[11], or other

---

[7] GDPR art 4(11)

[8] GDPR recital (43): "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."

[9] GDPR art 9(2): "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes" (emphasis added)

[10] GDPR art 7(3)

[11] GDPR art 9(2)(I): "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;"

substantial public interest[12]. Plainly the present situation would fit into such public interest categories. The requirements then are:

(a) a necessity test – that the public interest makes the processing of personal data necessary;

(b) safeguards in law – member state law providing suitable and specific measures to safeguard rights and freedoms.

As to the necessity test, the threshold is high: "necessary" is a strong word. In the UK Supreme Court Lord Kerr recently characterised this as meaning "strictly necessary"[13]. It involves a proportionality analysis[14]. Lord Sumption in the Supreme Court has said that a proportionality assessment involves considering whether a less intrusive measure could have been adopted without unacceptably comprising the objective[15]. Granted the availability of the decentralised Apple/Google scheme, the challenge then for NHSX is to demonstrate that only the centralised scheme can achieve the public interest objectives.

Even if that is achieved, NHSX will face, as matters stand at present, more problems with the requirement for a UK law providing specific measures to safeguard the rights and freedoms of data subjects. Such might be supplied by Professor Edwards' draft Bill; but there is no indication of Government interest in adopting it. Almost every commentator has urged the Government to enact specific safeguards, and to establish an oversight authority. To do so would not only assist in holding off legal challenges: it would also contribute to the sense of public trust, which could assist an app scheme to attain sufficient numbers of users to produce a useful outcome.

Transparency and Fundamental rights

Yet a further legal challenge for NHSX is to satisfy the first data protection principle, which is that the processing of personal data must be not only lawful and fair, but also transparent. Partly to satisfy transparency the GDPR requires that a Data Protection Impact Assessment where processing is likely to result in a high risk to the rights and freedoms of individuals. NHSX published such an Impact Assessment on the eve of the going live of its app in the Isle of Wight. Unfortunately this Assessment has not met with approval from specialists in the field. In a searing critique[16] Dr Veale has described it as "legally misleading", internally contradictory, "confusing" and involving the denial of the right of erasure without a specified legal reason for doing so.

The potency of the data protection law was dramatically demonstrated by the saga mentioned above about Google and the browser generated information. A group of computer users complained about Google accessing details of their internet usage. They had suffered no financial loss, but claimed general damages for distress and anxiety. The Data Protection Act 1998, which was then the governing statute in Britain, by s.13(2) specifically excluded the recovery of general damages by a claimant who had suffered no financial loss. The Court of Appeal was persuaded that the EU Directive, which was given effect by the Act of 1998, had intended to require the possibility of general damages in all cases;

---

[12] GDPR art 9(2)(g): "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"...

[13] *R (El Gizouli) v Home Secretary* [2020] 2 WLR 857 at [158]

[14] *Guriev v Community Safety Development* [2016] EWHC 643 per Warby J at [45]

[15] *Bank Mellat v HM Treasury* [2014] AC 700 at [20]

[16] "Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment 9th May 2020 at https://mcusercontent.com/3450ca9a08011894f4d1d5f7b/files/364c836f-4633-4a8d-86e6-44f5a985becb/Analysis_of_NHSX_DPIA.pdf , accessed on 13th May 2020

and that accordingly the Act had failed effectively to transpose the EU Directive into domestic law. Such inadvertent failure to transpose do happen. Sometimes the situation can be dealt with under the so-called *Marleasing* principle by interpreting an ambiguity in domestic law so as to achieve conformity with the EU instrument. On other occasions, the remedy has been so-called *Francovich* damages, that is a payment of financial compensation by the state for its mistake in implementation. But in this case, the Court was emboldened to "disapply", or in layman's language to strike down, s.13(2) of the UK statute by reason of the EU Charter of Fundamental Rights. The Charter contains a specific right to protection of personal data, and a right to an effective remedy. The Charter ceased to be a part of domestic law on 31st January 2020[17]; but there remain in domestic law until the implementation day[18] both the general principles of EU law, of which one is the right to an effective remedy, and the fundamental rights of EU law, which include those of data protection.

Fundamental rights considerations do not depend on EU-derived law. The European Court of Human Rights has on several occasions[19] held that the collection by the state of data about an individual engages the right to respect for private life in art 8 of the European Convention on Human Rights. All these fundamental rights factors may be expected to lead a court to subject the NHSX scheme to anxious scrutiny. Although I have set out the legal challenges to NHSX as distinct topics, they are closely connected with the first concern, that of fundamental principle. Ultimately, they may be seen as the black letter manifestations of an underlying unease of political principle about the scope which we may be creating for state surveillance.

Practical Drawbacks

A third ground for concern is that, quite apart from legality issues, and even if there is no mission creep, there exist real practical drawbacks of the NHSX scheme. In opting for a centralised app – if the Government really is to persist in doing so – the UK will be taking a different path from many, and probably most, other Western countries. Although France is planning a centralised app, the drift of thinking in Western Europe, both in countries who are EU members and others who are not, is towards a decentralised app. Notably, Germany, which was originally working on a centralised app, has after deeper investigation decided to use the Apple/Google protocol. Switzerland, Austria and Ireland are other countries to have announced a similar policy. It is being suggested that the USA is inclining the same way.

The Data Protection Commissioner for the Council of Europe has expressed a firm preference for a system based on "storing data on devices of the individual users", in other words the decentralised system. His statement adds the further judgment that no centralised system prevents the vulnerabilities and risks of re-identification, that is the revealing of the identity of individuals who have reported a diagnosis to the central authority.

Indeed, one may wonder whether the NHSX model will even command support from all the territories of the UK. The NHSX unit appears to be composed of the NHS of England and the government department whose health responsibilities are for England alone. Health is, of course, a devolved competence. Some of the devolved institutions have a keen attachment to rights, as well as, perhaps, a fondness for opportunities to go their own way.

---

[17] S.5(4) EU Withdrawal Act 2018
[18] S.5(5) EU Withdrawal Act 2018
[19] *S and Marper v UK* 48 EHRR 1169. The case concerned the retention of biometric data of persons who had been suspected of an offence but not convicted – a policy of the Labour Government which was stopped by the ncoming administration under David Cameron.

A practical consequence of divergence from other countries is a difficulty in interoperability.

The Parliamentary Joint Committee asked Mr Gould about the evidence it had heard. He did not deny the existence of the problem:-

> "We are worried about interoperability, so we have convened international partners to look at interoperability and to work out how we can make sure that it works best across borders. These things are never straightforward; to try to get these complex new systems on the new technology or to talk to one another will be no small task. The point is a good one, and we are trying to work through how it can best work."

Another problem on the international plane is that the NHSX scheme invites a user to self-report upon the development of symptoms. Almost every other Western country will require a Covid-19 diagnosis confirmed by a positive test. The European Commission has advised[20] that a notification of infection should require a diagnosis from an authorised health authority or laboratory -- in other words, a test result, not self diagnosis. This policy is to avoid a proliferation of false alerts, which would unnecessarily worry recipients of alerts and cause unnecessary self-isolations. It has been suggested that a UK scheme based on self-reporting might, therefore, lack international respect or acceptance as based on reliable data.

In a webinar held on 13th May 2020 by the Society of Conservative Lawyers Dr Veale explained that the only reason the NHSX model does not currently identify the individual who self reports infection is that this functionality has not been inserted as part of it, but that it would be "effortless", in other words easy, for somebody to design this into the NHSX protocol. He further said that there is a "high" risk of a hacker using Bluetooth technology to ascertain the identity of a user of the NHSX app. So technical weaknesses in the NHSX system is a further practical drawback.

[20] "Mobile Applications to Support |Contact Tracing in the EU's fight Against COVID-19" 15th April 2020 at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf accessed on 13th May 2020

III

Next Steps

Many of the questions raised by the use of the NHSX are already being considered by MPs. The Joint Parliamentary Committee on Human Rights has proposed delays and safeguards. Others have drawn attention to the introduction by other countries of a non-centralised app for some of the reasons discussed here. The government, meanwhile, has started its pilot scheme on the Isle of Wight and though continuing with the centralised model, it is keeping 'all options under review to make the app as effective as possible' (8 May).

Prompted by the concerns discussed in this analysis, the Joint Committee on Human Rights has advised that the Government should not rollout the NHSX app until important steps have been taken[21]. These include the enactment of legislation to provide assurances on privacy, and the establishment of a Digital Contact Tracing Commissioner to oversee it. The Committee calls for the highest standards of data security, and for the deletion of all data at the latest after 2 years. It seems that all these sensible suggestions are being ignored. Government sources today are seemingly briefing the press of an intention to roll out the NHSX app nationally during the present month of May.

There are strong reasons now to move to other options. All in all, the NHS app is an unnecessary mare's nest of problems. Our heritage leans heavily against a powerful or all-knowing state. For example, Britain is a country, which unlike most of our European neighbours, has always resisted identity cards in peacetime. A centralised contact tracing app may reflect the centralised organisation of the NHS: but it fits ill with the deeper political culture of our nation. If to be deployed at all, it must be delayed until safeguards, such as those in the Edwards draft Bill have been enacted. But the better course will be to abandon NHSX, and in common with most of the rest of the Western world use the safety of a decentralised tracing model.

[21] https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/34302.htm

Subscribe to Politeia's Publications!

For £35 a year you will receive an electronic copy of each of our publications, plus hard copies of two new publications on request, and, if you wish, free hard copies of your choice from our back catalogue. You will also receive advance notice and invitations to Politeia's conferences and flagship events, with guest speakers from the UK and overseas.

More information can be found on our website: www.politeia.co.uk. Or, write to the Secretary, Politeia, 14a Eccleston Street, London SW1W 9LT, or at secretary@politeia.co.uk

A Selection of Recent and Related Publications

How to Level the EU's Playing Field-Trade Remedies for a Trade Deal
David Collins

Managing Euro Risk: Saving Investors from Systemic Risk
Barnabas Reynolds, David Blake and Robert Lyddon

All Change? UK State Aid after Brexit: What Law? What Courts?
James Webber

Now or Never: Countering the Coup Against Britain's Democracy
Sheila Lawlor

Leave as You Entered: Brexit in International Law
Thomas Grant

The Battle for Western Civilisation and the Origins of Western Philosophy
John Marenbon (with New Direction)

Any Role to Play in UK Law? The EU Charter of Fundamental Human Rights
Anthony Speaight QC

UK and EU Financial Services: The Legal Framework for Free Trade After Brexit
Barnabas Reynolds (with New Direction)

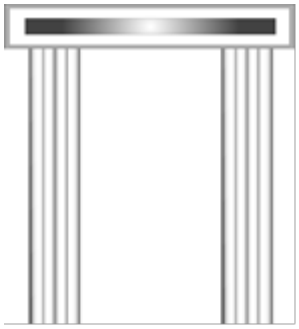
Avoiding the Trap – How to Move from the Withdrawal Agreement
Martin Howe QC, Richard Aikens and Thomas Grant

The EU, the UK and Global Trade – A New Roadmap
David Collins (2nd edition, June 2019, with New Direction)

Intangible Assets: Funding Research in the Arts and Humanities
John Marenbon (with New Direction)

The British Bill of Rights: Protecting Freedom Under the Law
Jonathan Fisher QC

What's the Point of the Human Rights Act:
The Common Law, the Convention, and the English Constitution
Dinah Rose QC



…

POLITEIA