36 COMMERCIAL

COVID-19 ASSISTANCE HUB

THE LEGALITY OF THE USE OF MASS SURVEILLANCE DATA TO CONTAIN THE COVID-19 OUTBREAK

Introduction

The COVID-19 pandemic is likely to precipitate a number of measures that will impact on ordinary rights and freedoms. In this note we examine the legality and ramifications of "contact tracing", first, in the context of data protection and, second, in the context of privacy rights.

Data protection

What does "contact tracing" entail?

"Contact tracing" involves identifying infected people, isolating them and then tracing anyone that the infected person has had contact with.

South Korea is probably the country that has had the most success in containing the outbreak of COVID-19.[1] The South Korean government used an aggressive "contact tracing" approach to containing the virus. They conducted random mass testing, identified infected individuals, isolated those individuals and then trawled security through camera footage, phone location data and credit card data to identify people

[1] https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

that they had come in to contact with. This information was relayed to the South Korean public by smartphone apps and websites to alert them to the fact that they had come in to contact with an infected individual and that they needed to be tested.

.

South Korea managed to contain COVID-19 with relatively modest social distancing measures as opposed to the draconian lockdowns that we have seen in so many parts of Europe and the United States. Most importantly, South Korea had a very low fatality rate from COVID-19 as a result of the strategy that it adopted.

This South Korean approach was born out of hard lessons learned by South Korea in the SARS and MERS outbreaks that many other western countries had been spared.

A similar strategy appears to have proven successful for China in containing the virus outside of Wuhan.

The United States and many governments in Europe are now exploring adopting similar technologies in the hope of containing the virus and reducing fatalities. Google and Apple are working collaboratively on an opt-in contact tracing tool that will use blue tooth technology, and in conjunction with mass public testing, will tell smartphone users whether they have been in contact with someone infected by COVID-19 at a distance of 6 feet or less for 15 minutes or more, where that other person is also carrying a smartphone using the same tool.[2]

If the use of this technology in conjunction with widespread public testing for COVID-19 in western societies is as successful as it was in South Korea, it would allow for greater containment of COVID-19. Most importantly, this would mean fewer fatalities. It would also likely mean more modest social distancing measures and reduce economic damage.

---

[2] Details about the tool are still scant at this stage. It appears that Google and Apple are building the tool in to their respective smartphone operating systems and app developers will build contact tracing apps on top of this: https://techcrunch.com/2020/04/13/daily-crunch-apple-and-google-announce-contact-tracing-initiative/ and https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health

The South Korean government was able to conduct this mass surveillance because its data protection regime provides for an exemption from their data protection regime for the temporary processing of public data in relation to public health / a pandemic.

At first blush, the blue tooth technology that Google and Apple propose to use appears far less intrusive than the technology being used by South Korea and China.[3]

But the question in the UK is how this would be regulated by the Data Protection Act 2018 (DPA).

Could mass surveillance data used by the government fall outside the data protection regime on the basis that it was anonymised?[4]

First, anonymising data is a very high bar and it is difficult to achieve. Hashing data is generally not sufficient. Often there is a way to reverse engineer "hashed" data such that an individual can be identified.

Even if it were possible to anonymise the data, it is still likely that an individual could be identified if a government department were to publish a "virus travel log" of an infected individual's travel path on the internet, even without naming that individual. Someone, somewhere (e.g. a close friend or relative) is likely to be able to identify the individual from the published travel path. Anecdotally, one man in South Korea was accused of having an extra-marital affair because of the publication of such information.

However, a mere notification on a mobile phone app that a user had come into close contact with an infected individual would be far less likely to suffer from this problem (although, as set out in the next section, they may still be a privacy issue). Google and Apple appear to be heading down this path with their new contact tracing tool.

---

[3] https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health

[4] Recital 26 of the General Data Protection Regulation (EU) 2016/679 (GDPR) states that GDPR is not applicable to anonymised data

Nevertheless, it would still be possible for someone processing the data, likely a government department, to identify an individual using that data even if it was "hashed".

In sum, it is challenging to anonymise mass surveillance data such that it would not be subject to GDPR.

Could the government classify the pandemic as relating to "national security"?[5] If it could, what are the DPA implications?

The term "national security" would normally relate to foreign intelligence or military threats to UK sovereignty or the safety of its citizens, rather than a pandemic.

If the pandemic was so classified, the Government would simply have to show that the processing was "lawful" and would not be subject to other more stringent requirements of the data protection regime.[6]

However, the references to a partial exemption from the data protection regime for "public health" in the GDPR and DPA makes it more likely that a court would deal with "contact tracing" as falling more naturally within the "public health" partial exemption,[7] rather than the "national security" exemption.

On the basis that a pandemic is a matter of "public health" what requirements of the DPA would apply in relation to mass surveillance conducted by the government?

The general requirements of Article 5 of the GDPR would apply to both the Government or third parties assisting the Government use mass surveillance data for aggressive "contact tracing". The general requirements of Article 5 of the GDPR are that mass surveillance data must be processed:

1. Lawfully, fairly and transparently;

---

[5] Section 26 of the Data Protection Act 2018 (DPA 2018); see also recital 16 of the GDPR

[6] See particularly section 26(1) and 26(2) of the DPA 2018

[7] This would be a matter of statutory interpretation having particular regard to Article 23 of the GDPR. In these authors' view, it is clear that a data processing in relation to a pandemic would fall within a matter relating to "public health" as it is the most specific exemption in that Article.

2. In a manner consistent with the purpose minimising the spread of COVID-19;
3. Limited to what is necessary to minimise the spread of COVID-19;
4. Accurately.
5. Kept for no longer than is necessary;
6. Security / confidentiality of the data must be maintained.
7. The Government must be able to demonstrate compliance with all of the above principles.

Does the Government need the consent of an individual to use their phone location data to contain the spread of COVID-19?

The short answer is no.

One possible way of demonstrating a lawful purpose for using mass surveillance data is by the government obtaining a user's consent.[8]

This appears to be the UK government's favoured route: It has been said that the use of mobile phone apps will be voluntary. Presumably, it will ask for the consent of the user to share their location data and "opt-in" to the aggressive contact tracing regime. From a public health point of view, the concern with going down this road is that many users may not "opt-in" to sharing location data / Government surveillance. Anecdotally, only 12% of the population in Singapore "opted-in" to these contact tracing smartphone applications.[9] At that level of adoption, an aggressive contact tracing strategy using smartphone technology would unlikely to be effective.

However, the Government could adopt a more coercive approach if it desired. Lawful purpose can be established pursuant to Article 6 of the GDPR by showing that the processing is necessary for an individual / another person's vital interests or is otherwise in the public interest.[10] It is therefore not strictly necessary for the

[8] Article 6(1)(a) of the GDPR

[9] https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health

[10] Article 6(1)(d) and 6(1)(e) of the GDPR

Government to obtain an individual's freely given consent[11] to demonstrate "lawful purpose" in relation to a pandemic.

If it desires, the Government could require individuals to download and install a mobile phone app before, say, using public transport, if this assisted the Government in its aggressive "contact tracing" strategy for the purpose of containing the spread of COVID-19.

The Government could also make use of an individual's mobile phone location data without their knowledge if this was necessary to try and contain COVID-19, provided it abided by the 7 principles outlined above. However, it appears that the tools that Google and Apple are developing are not likely to allow such an approach. This is not a great surprise in the wake of data protection concerns in the wake of the Cambridge Analytica scandal and privacy concerns more generally.

What are the risks of mass data surveillance?

In South Korea, the Washington Post has reported that one coronavirus patient whose travel history was released has filed proceedings concerning the violation of his privacy to the National Human Rights Commission.

There are very real risks that the Government could be sued if it does not comply with the 7 principles outlined above.

The DPA and oversight of any mass surveillance program by the UK Information Commissioner's Office should hopefully alleviate these concerns in the UK.

We already accept draconian lockdown laws that severely inhibit freedom of movement and freedom to conduct business by individuals. While the use of mass surveillance data creates concerns about how that data might be used and will result in a loss of privacy, if done responsibly, it may actually prove an effective way to reduce fatalities and have the added benefit of more modest social distancing measures than those we currently have to live with.

[11] See particularly recital 32 of the GDPR in relation to what constitutes "consent"

Privacy

The English common law is alone, amongst comparable democracies and other common law jurisdictions, in lacking a comprehensive and general law of privacy.[12] The United States of America has it; New Zealand and Australia have it; the Roman Dutch law jurisdictions of Southern Africa (nevertheless much influenced by the common law) have it; Canada has it; so do most European Union countries with France and Germany to the forefront. The protections are not all the same, and many have been spurred by statutory instruments such as Canada's Charter Of Rights And Freedoms, the US Constitution, South Africa's Constitution or the European Convention on Human Rights, but these jurisdictions all recognise privacy as a basic right and all protect it as such.

There are, however, various forms of invasion of privacy that give rise to a legal remedy in English law, but these have not developed logically or consistently, leading the authors in Markesinis and Deakin's *Tort Law* (8th Ed 2019) to these conclusions:

> "… Gaps in protection are largely the result of a piecemeal and gradual process of development, the result of which is a set of protections that is patchy, unprincipled, and, arguably, dangerously complex …"[13]

And:

> "The damnation of our law thus comes more from the persistent attempts of English Judges to afford such protection as they see fit by means of expanding medieval torts by putting them on a procrustean bed and stretching them in a way that satisfies neither modern logic nor contemporary feelings of justice."[14]

The Human Rights Act, 1998, gave effect to certain rights and fundamental freedoms guaranteed under the European Convention on Human Rights, Article 8(1) of which

---

[12] *Wainwright and Ano v The Home Office* [2003] YKHL 53.

[13] At p 695.

[14] At p 706.

provides that “everyone has the right to respect for his private and family life, his name and his correspondence.”

This has nudged the courts into slowly recognising rights of privacy in certain situations : so a tort bearing the clumsy moniker, “misuse of private information”, now exists to protect information where there is a reasonable expectation of privacy.[15]

Over and above private information, courts have recognised, in at least two cases, a person’s right to privacy in a public place taking into account certain circumstances, some of which (ie. the attributes of the claimant, the effect on the claimant, and the age of the person) are plainly irrelevant because anyone can entertain a reasonable expectation of privacy even in a public place.[16] They have also recognised a right to anonymity orders in court proceedings derived from the Article 8 Guarantee of Private and Family Life, but only subject to any public interest in publication.[17]

Glaring omissions in English cases include the lack of any remedy for the government interception of electronic communications[18] and also of intrusion into an obviously private space such as a hospital ward.[19] The vulnerability of the decisions in *Malone* and *Kaye* to attack and reversal in these times of heightened sensitivity regarding privacy and data issues, is illustrated by the willingness of the South African courts, over a very long period of time, to protect privacy in similar and analogous cases.[20]

---

15 *Campbell v MGN Limited* [2004] 2 AC 457 (HL) at [14] and [11]

16 *Murray v Express Newspapers Plc* [2007] EWHC 1908 (Ch.); *Weller v Associated Newspapers Ltd* [2015] EWCA Civ. 1176

17 *In re Guardian News and Media Ltd* [2010] 2 AC 697

18 Where the position is apparently still that set out in *Malone v Metropolitan Police Commissioner* [1979] Ch. 344

19 Where the position is apparently still that set out in *Kaye v Robertson* [1991] FSR CA

20 *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (AD) (unauthorised bugging of a telephone and publication of the information so acquired).
S v A and Ano 1971 (2) SA 293 (T) (bugging a person’s apartment to obtain evidence of adultery).
Janit and Ano v Motor Industry Fund and Administrators (Pty) Ltd and Ano 1995 (4) SA 293 (AD) (theft of tape recordings of board meetings and disclosure of information contained therein).
R v Holliday 1927 CPD 395 (peeping at a woman while she was undressing).
S v I and Ano 1976 (1) SA 781 (RA) (entry into a private residence)
Reid-Daly v Hickman and others 1981 (2) SA 315 (ZA) (reading another’s documents).
Epstein v Epstein 1906 TH 87 (shadowing a person)

The limiting principles to these emerging rights appear to be, first, whether there can be a reasonable expectation of privacy and, second, whether issues of public interest trump any right to privacy that may otherwise be found to exist.[21] In this regard, any measures taken to meet a particular emergency or crisis would, at least where the right to privacy has a constitutional or statutory status, generally be required to be necessary in a democratic society.

Strangely, there have been no cases in which the UK government has been held to account for invasions of privacy and therefore a breach of section 8(1). Any barrier to such litigation may well buckle under the pressure of public concern over mass surveillance tactics should they eventuate. The English courts may then look to how the US courts enforce the constitutional right to privacy against government interference : in that jurisdiction, for example, law enforcement officers enabled by a warrant to enter and search premises, and accompanied by the media, acted unlawfully because the presence of the latter constitutes an invasion of privacy;[22] and the use of thermal imagery equipment by the authorities to detect a marijuana factory in a home was an invasion of privacy.[23] Also relevant, may be South African decisions, both by the Constitutional Court and in the pre-constitutional era, holding that a person's medical condition is a private fact and disclosure can attract a damages award or injunction.[24]

What may be taken from these cases is that private communications and private activities, albeit in public places such as a road or a shopping centre, and movement between public places, are either ordinarily protected from monitoring and disclosure, or at least may very arguably be so. This would certainly include the mass surveillance described above and all monitoring of individuals, disclosures of their coronavirus status as well as all contact tracing consequent upon such surveillance.

---

[21] *Hutcheson v News Group Newspapers* [2011] EWCA Civ. 808; *Ferdinand v MGN Ltd* [2011] EWHC 2454 (QB)

[22] *Wilson v Lane* 526 U.S. 603, 1999

[23] *Kyllo v United States* 533 U.S. 27

[24] *NM and others v Smith and others* 2007 (7) BCLR 751 (CC)
Jansen van Vuren and Ano NNO v Kruger 1993 (4) SA 542 (AD)

On the other hand, however, the qualifications built into privacy laws wherever they are found would, in all likelihood (save perhaps in the US), have the effect of authorising these actions by the relevant authority, perhaps subject to safeguards that would render the qualification necessary in a democratic society. The defence of public interest is the obvious qualification in this regard, but it may also be an interesting (and difficult) question as to whether or not citizens actually can have a reasonable expectation of privacy in the face of a crisis; potentially such an expectation may be held by courts to have been compromised by the magnitude of the crisis.

John Campbell SC
Ben Symons

36 Commercial

T: +44 (0) 207 421 8051

E: clerks@36commercial.co.uk

W: https://36group.co.uk/commercial