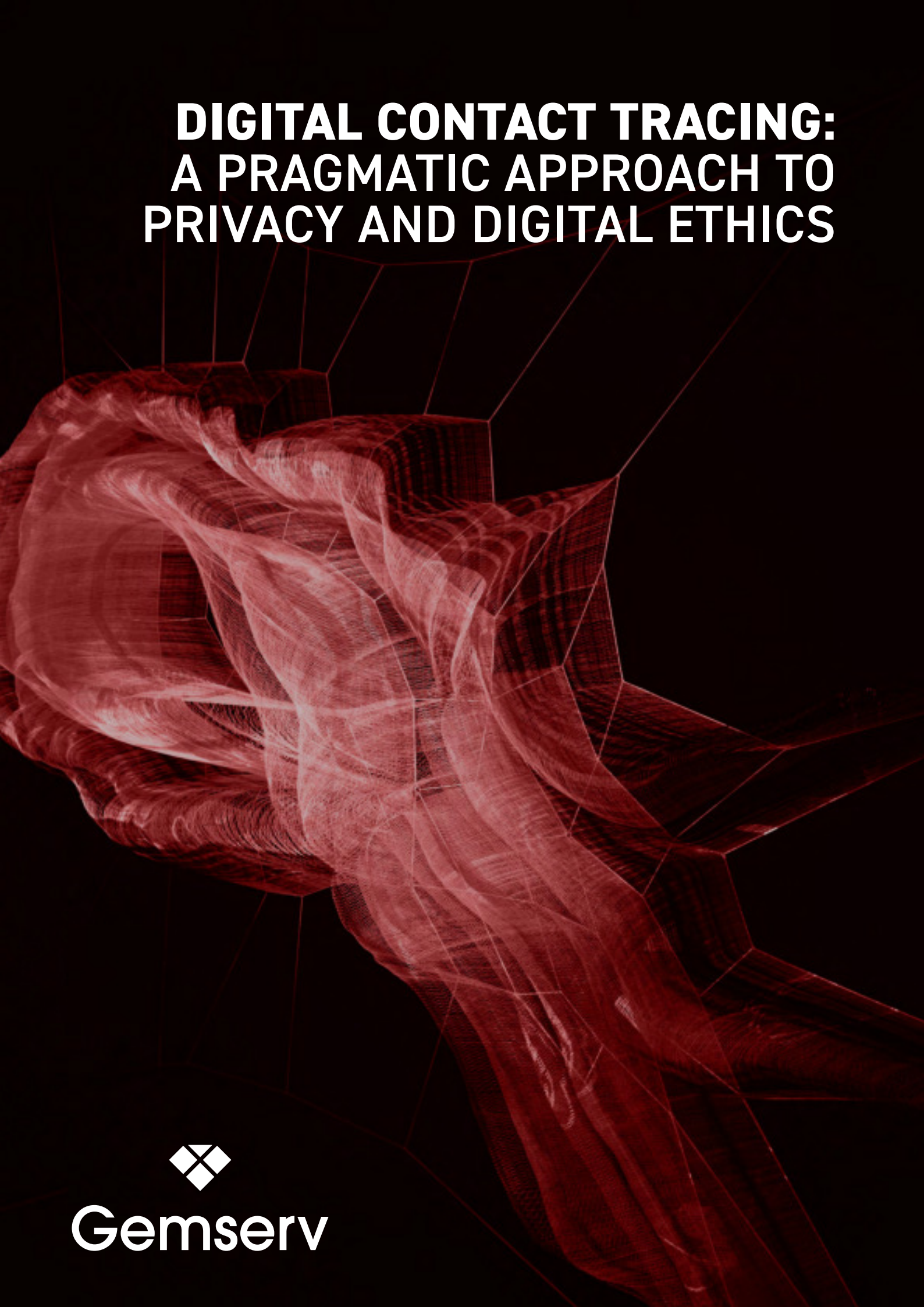
DIGITAL CONTACT TRACING: A PRAGMATIC APPROACH TO PRIVACY AND DIGITAL ETHICS



Gemserv

DIGITAL CONTACT TRACING

The COVID-19 contact tracing apps have made the headlines recently and have been a widely debated topic, especially among privacy professionals. Countries around the world have rushed to launch their contact tracing apps as part of their wider efforts to curb the spread of the COVID-19 and ease lockdown. Different countries have adopted their own strategies and contact tracing technologies, ranging from the use of proximity Bluetooth tracking, to geo-location, and facial recognition.

According to the COVID-19 Digital Rights Tracker, as of 13 May 2020, in response to the pandemic:

- "Contact tracing apps are being used in 28 countries;
- Alternative digital tracking measures are in use in 32 countries;
- Physical surveillance technologies are in use in 10 countries;"

In the UK, the Government has published its COVID-19 Recovery Strategy Plan as a roadmap to respond to the crisis.

The NHS launched its COVID-19 contact tracing app in the Isle of White on a pilot basis last week. The app will be part of a wider approach that will involve contact tracing and testing as per the NHS research arm.

It is now reported that NHSX is working on a second contact tracing app following concerns around privacy.

The NHS is aiming to use this digital tool to reduce the transmission of COVID-19 by making people aware when they are at the risk of an infection and the actions they need to take to protect themselves, their loved ones and the NHS. The NHS also considers it to be an important measure to ease lockdown.

A contact tracing app, along with other strategies, present the opportunity to the Government to meet the goal of protecting lives as well as gradually lifting the restrictions gradually to help kickstart our stagnated economy until a vaccine is available. If approached and implemented by following the core data protection principles, it can set a clear path for achieving good data governance while also promoting transparency, accountability necessary for trustworthiness, and safety for each and every one of us in this crisis time.

A contact tracing app also processes large volumes of data, including personal data, some of which may be sensitive. If it is not approached and implemented in the right way, the right to privacy and data protection concerns will be paramount and this can affect the value that can be derived from the initiative.

The NHS, the Government, regulators, privacy experts, and ethicists involved are definitely tasked with an extraordinary intervention in this extraordinary time: balancing data protection and right to privacy with the urgent need and pressure to fight the Coronavirus, ease lockdown and bring the economy back.

We welcome the approach that the NHS has taken to develop its app "in consultation with the Information Commissioner (who is going to support the NHS throughout the lifecycle of the app), the Centre for Data Ethics and Innovation and representatives from Understanding Patient Data and volunteers who provide a patient and public perspective".

It also crucial that experts in the medical and scientific field are consulted to support the usefulness and efficiency of the solution and as per the NHS, it seems that scientists and doctors are supporting "to fine-tune the app to ensure it is as helpful as possible both to individuals and to the NHS in managing the pandemic."

In this difficult time, it is reassuring to know that the standards of data protection, data security, and even ethics have been considered as a working foundation.

This is a good start. However, more actions will need to be taken so that public trust can be won throughout, and the technology is widely adopted to help fight the pandemic in a meaningful way as intended.

Decisions taken now will have lasting effects, so long-term privacy and civil liberties impacts must be considered to get this right, and there is only one chance to get this right!

DIGITAL CONTACT TRACING

Following the core data protection principles will set sail in the right direction:

1. Keeping the use of a contact tracing app voluntary – The systematic and large-scale monitoring of location and/or contacts between people involves the processing of very sensitive personal information. As such, the processing of such data will be lawful if a user voluntarily adopts the use of a contact tracing app based on clearly defined purposes. Those who ultimately decide not to do so, must not be penalised in any way.
2. Transparency – Clear information on the processing of personal data by a contact tracing app must be provided to users in a plain language, covering the identity of all the controllers involved, the purposes for which personal data will be processed, the categories of the personal data, most importantly, the recipients of the personal data. Publishing the source codes as will help promote transparency and gather independent opinion on the security of the app but backend information about what happens to NHS servers must also be published.
3. Purpose limitation – It is crucial that data is not used for purposes by those whose mission is not public health related. The purposes must be specified and explicit enough to exclude further processing for purposes not related to the management of the COVID-19 crisis, such as commercial exploitation or law enforcement purposes.
4. Data minimisation and data protection by design and default – A contact tracing app must avoid processing personal data that are not necessary for fulfilling the purpose, i.e., the management of the COVID-19 crisis. The design of the app and the contact tracing framework itself must support this principle.

At the moment, there is a big debate among privacy professionals on whether contact tracing apps must operate on a centralised or decentralised system. In Poland and in the UK, there is a preference for a centralised approach while other European member states are mainly interested in the decentralised approach.

Whilst each approach has its own pros and cons, they both present the capabilities to be compliant with data protection principles and have privacy implications as well. Also, the relationship of trust between the citizen and the app varies differently between the 2 approaches.

The types of personal data that are more likely to be processed for each approach have been listed below based on a study conducted by technologists:

KEY PERSONAL DATA CONCERNED	DECENTRALISED APPROACH	CENTRALISED APPROACH
(1) Proximity data	Processed	Processed
(2) Interaction data	-	Processed
(3) Location tracking of infected users	-	Processed
(4) Location tracking of non-infected users	-	Processed
(5) Percentage of infected people	Could be noise estimates only	Processed

The decentralised approach seems to be more privacy friendly and would comply with the data minimisation principle as its main objective is limited to notification only. The centralised approach seems to be less privacy friendly but may be more conducive if the aim is for epidemiologists to conduct studies and research, which should be subject to a proportionality test. The centralised approach requires careful deployment and maintenance. It also sets the standards of trust quite high to reassure users that this is not a step towards state surveillance.

DIGITAL CONTACT TRACING

As you can note, contact tracing involves the use of innovative technology, systematic monitoring, processing of special category of data such as health related data and sensitive information such as location data and large-scale processing. Conducting a comprehensive Data Protection Impact Assessment (DPIA) is mandatory before the deployment of a contract tracing app and publication of the DPIA is crucial for more transparency.

Furthermore, it goes without saying that a contract tracing app, its back-end servers or any associated services must be kept safe from cyber threats throughout their lifecycle. As such, on top of the DPIA, a cybersecurity focused risk assessment and testing must be conducted before deployment to mitigate risks and implement adequate technical requirements such as the use of encryption, secure communications, user authentication, incident response measures, among others.

6. Storage limitation – Also, as soon as possible, the criteria to determine when the data collected for COVID-19 purposes must expire must be explained, including which entity will be responsible for taking that decision. This is important to ensure that there is no compromise of constitutional civil liberties when we emerge on the other side of the crisis. All personal data must be retained only for the duration of the COVID-19 crisis as a general principle. After that, all personal data must be either erased or anonymised. This is even more important in the case where a centralised approach is adopted. Users will also need to be explained how easy it will be for the app to be dismantled and the likely impact on data collection if they do not or are not able to do so.
7. Accountability – Where the deployment of a contact app involves various actors with varying roles and responsibilities, the controllers and processors must be clearly identified from the beginning and their roles and responsibilities explained to the users of the app in simple language. This is important to comply with the principle of accountability in the General Data Protection Regulation (GDPR).
8. Auditability – Where a contact tracing app integrates an infection risk analysis algorithm, the algorithms must be auditable by experts. The application's source code must be published for wider scrutiny by privacy experts. This seems to be the intention of the NHS.

The likelihood of false positives or false negatives being generated by the app must be taken into account, for instance, in areas of high population density, identifying those in adjoining flats as being in close contact despite being separate by a wall.

False positives or false negatives of an infection risk is likely to have a high impact on a person, so it is important to consider those consequences and plan for the mitigation measures that will be implemented, such as the correction of data, results analysis, and the feasibility thereof.

Contact tracing has digital ethics implications as well and they need to be tackled before deployment:

Accessibility and Inclusiveness – The success of a contact tracing app will depend on a number of factors, including the number of people who can download it.

As per a letter sent by a group of technologists to the NHSX and the Government, "In the UK, OFCOM figures[1] show that 22% of UK adults do not have a smartphone, rising to 45% of adults over 55, and figures on device ownership for young children vary wildly." So, accessibility will be a challenge as we need 60% of the population to use the app actively for it to be an effective solution. The inclusiveness aspect comes into play for specific vulnerable data subjects like children, old people, patients who suffer from other illnesses and those who may have a hearing or vision impairment. They may have accessibility to a smart phone but probably, they do not have the necessary skills and knowledge to install an app from their appstore for instance. To prevent a digital divide, special measures must be implemented at a national level to support the use of the app, such as a customer service offering guidance, exploring the use of equivalent solutions compatible with the contact tracing system for those who do not have accessibility to smart phones, among others.

Ethically justifiable design – As pointed out in a paper released by the University of Oxford [2], "Interventions must be necessary to meet a specific public health objective, proportional to the seriousness of the public health threat, scientifically sound to support their effectiveness, and time-bounded".

The paper highlights that there should be a test performed on such technologies which assesses the existence of enabling factors which inform the design of a contact tracing app from an ethical perspective, such as the ability for users to have autonomy over their data, the extent to which their autonomy could be preserved, and the proportionate benefit in disease containment by the use of such technologies.

[1] Group of technologists, 2020, Open Letter: Contact Tracking and NHSX, viewed 28 April 2020, https://medium.com/@rachelcoldicutt/open-letter-contract-tracking-and-nhsx-e503325b2703

[2] Jessica Morley, Josh Cowls, Mariarosaria Taddeo, Luciano Floridi, 2020, Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems, Oxford Internet Institute, University of Oxford, The Alan Turing Institute, Oxford and London.

DIGITAL CONTACT TRACING

(Note '+' stands for what the ethicists consider to be a more ethical outcome and '–' stands for what they consider to be a less ethical outcome. DTT stands for Digital Tracking and Tracing Systems):

Questions to determine the extent to which a DTT is ethically justifiable

High-level Principles (answer the question: is the correct DTT system being developed?)

1) Is it a necessary solution?
   + Yes, the app must be developed to save lives.
   - No, better solutions are available.
2) Is it a proportionate solution?
   + Yes, the potential negative impact of the DTT system is justified by the gravity of the situation.
   - No, the potential negative impact of the DTT system is disproportionate to the situation.
3) Is it scientifically sound?
   a) Will it be effective?
      i) Is the timing 'right'?
      ii) Will adoption rates be high enough?
      iii) Will it be accurate?

   + Yes, evidence shows that the system will work, is a timely solution, will be adopted by a sufficient number of people, and yields accurate data and insights.
   - No, the app does not work well, arrives too late or too soon, will not be adopted extensively, and is likely to collect data that are insufficiently accurate (too many false positives and/or false negatives).
4) Is it temporary?
   + Yes, there is an explicit and reasonable sunset clause.
   - No, its deployment has no defined end date.

Enabling Factors (answer the question: is the DTT system developed correctly?)

5) Is it voluntary?
   + Yes, it is optional to download and install the app
   - No, it is unnecessarily mandatory and sanctions may be applied for non-compliance
6) Does it require consent?
   + Yes, people have complete choice over what data are shared and when, and can change this at any time
   - No, the default data settings of the app are to share everything all the time and this cannot be altered.
7) Are the data kept private and users' anonymity preserved?
   + Yes, data are completely anonymous, held only on the user's phone. Others found to have been in contact are only notified that there is a case of contact at risk of contagion, not with whom or where the contact took place. Methods such as differential privacy are used to guarantee this. Cyber-resilience is high.
   - No, data are completely (re)identifiable due to level of data collected, and stored centrally. Locations of contacts are also available. Cyber-resilience is low.
8) Can the data be erased by the users?
   + Yes, users can delete data at will, and in any case all data will be deleted at sunset (see 4).
   - No, there is no provision for data deletion or guarantee that it can ever be deleted.
9) Is the purpose defined?
   + Yes, it is clearly defined, the app notifies individuals only when they have been in contact with people with confirmed infection, and only essential data are collected (e.g. confirmed health status and time of contact).
   - No, terms and conditions are loosely defined, there is no guarantee that data will not be used for secondary and only loosely related purposes, data collected may also be combined with other databases. Multiple data sources may be collected, without any transparency, with no user control.
10) Is the purpose limited?
    + Yes, the app is used for personal monitoring purposes only.
    - No, the app can be regularly updated adding extra features that extend its functionality, e.g. for future studies about pandemic risks.
11) Is it used only for prevention?
    + Yes, the app is used only to enable people voluntarily to prevent spread ("flattening the curve").
    - No, the app is also used as a passport, e.g. to enable people to claim benefits or return to work ("support phase two").
12) Is it used to monitor users' behaviour?
    +No, the app is not used to comply with any required behaviour.
    - Yes, the app is used to monitor behaviour
13) Is it open-source?
    + Yes, the source code of the app is made available, so all aspects of design can be inspected, sharing is supported, and collaborative improvements are facilitated.
    - No, the source code of the app is unavailable, and no information about it is provided in any other form.
14) Is it equally available?
    + Yes, the app is freely and widely distributed to anyone who wishes to download it and use it.
    - No, the app is arbitrarily given only to selected users.
15) Is it equally accessible?
    + Yes, the app is freely and widely distributed to anyone who wishes to download and use it.
    - No, only those with specific mobile phones, part of specific digital ecosystems, and with sufficient digital education can use the app.
16) Is there an end-of-life process to retire the system?
    + Yes, there is a clear road map to deal with the app being officially decommissioned.
    - No, there are no policies in place to manage the final stage of maturity of the app.

The above seem to resonate with the principles we have outlined.

While technology presents many opportunities, we need to acknowledge that it also has its own limitations. There is a tremendous amount of work for the NHS and the Government to do to get this right in limited time. The stakes are high as the use of a contact tracing app must not be a backdoor to mass surveillance. Trust will be the key enabler for bigger return. Treading carefully by following the measures outlined as a threshold will go a long way in carving out a good 'new normal'.

Gemserv

Gemserv

Gemserv

LONDON

+44 (0)20 7090 1022

bd@gemserv.com

IRELAND

+353 (0)1 669 4630

ireland@gemserv.com

CONTACT US TODAY, TO DISCOVER HOW WE CAN HELP YOU