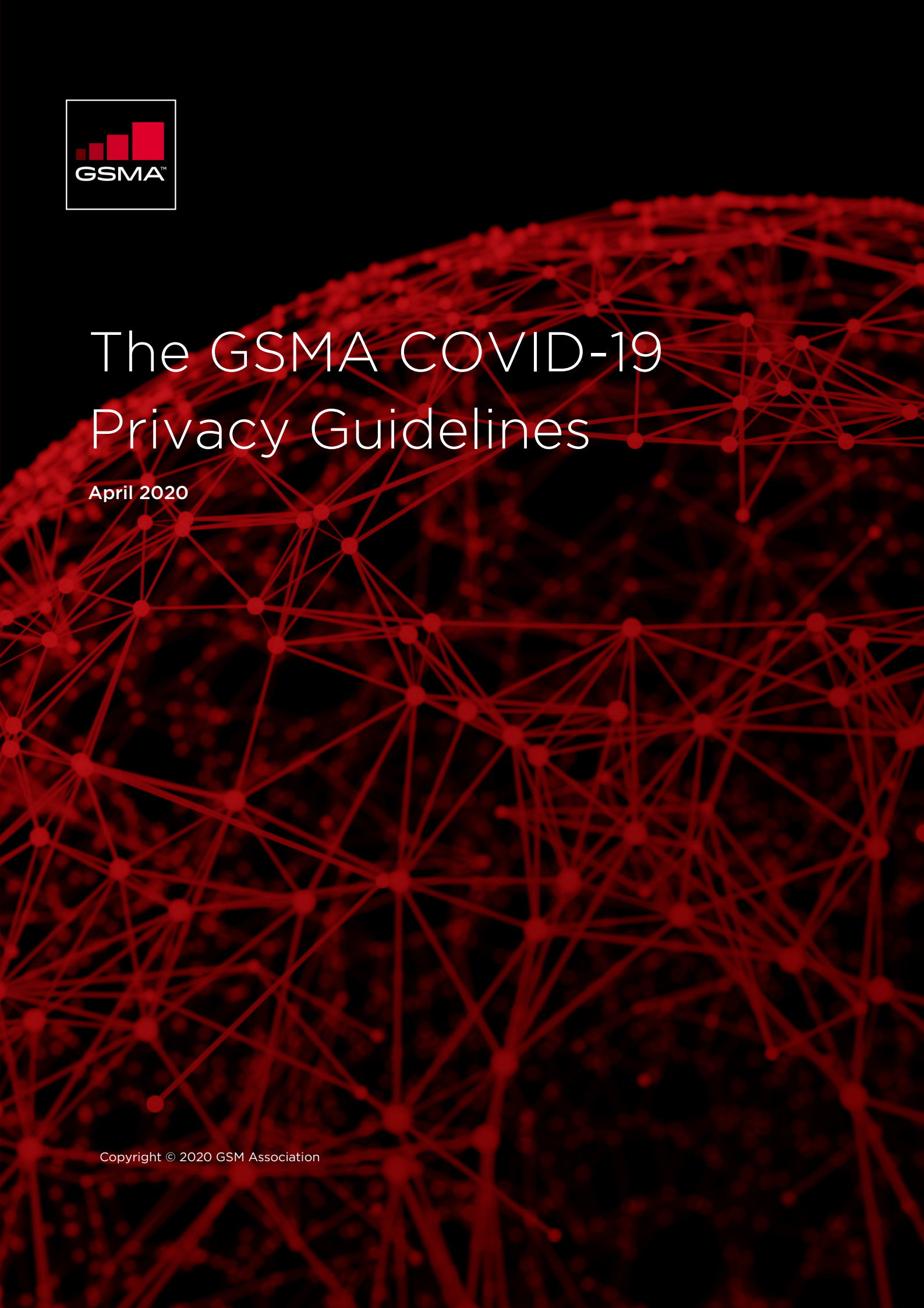

The GSMA COVID-19 Privacy Guidelines

April 2020

Introduction

As COVID-19 continues to spread rapidly in many parts of the world, some governments and other agencies are making requests for data or insights held by mobile network operators (MNOs) and other companies.

Data and insights from mobile networks and other internet companies could be important because mobility of people is one of the critical factors that contribute to the spread of human-transmitted infectious viruses. Accurate, up to date information on aggregated mobility patterns could be potentially vital for monitoring, predicting outbreaks, and planning future resource needs such as testing kits, beds, medical staff, or equipment. Other use cases may include identifying people who may have been in contact with confirmed cases, or informing people if they have entered an affected area provided that this would be in accordance with the law.

The mobile industry recognises the urgency with which governments must act to slow the spread of COVID-19 and the desire of some governments to seek help regarding those efforts. At the same time, the mobile industry recognises that the use of mobile network operator data by governments or agencies raises serious privacy concerns. These guidelines reflect recommendations on how the mobile industry may maintain trust while responding to those governments and public health agencies that have sought assistance in the fight against COVID-19.

Key terms used in these Guidelines:

'Metadata' means traffic data including call detail records[1] from mobile networks including where key identifiers such as the mobile number and subscriber information have been replaced with a pseudonym[2].

'Aggregated Non-Identifiable Data' means Metadata in an aggregated form with appropriate thresholds (for example, regarding the number of individuals, time and/or space) designed to prevent the possibility of individuals being re-identified. This typically includes origin-destination matrices or footfall information generated from Metadata. Although every effort is made to avoid the possibility of re-identification in the way these datasets are designed, there remains a residual, theoretical risk making it difficult to pass the legal test of true anonymity imposed in some jurisdictions.

'Insights' means the product, dashboard or visualisation of analytics carried out on Aggregated Non-Identifiable Data.

'Mobile Operator Data' means any or all of the above definitions for Metadata, Aggregated Non-Identifiable Data and Insights.

'Governments or Agencies' includes governments, public health authorities and other agencies such as UN agencies, international and intergovernmental organisations or regional bodies that seek access to

[1] Call Detail Records (CDR) data – a record of a voice call or other transaction e.g: SMS generated by a mobile network operator that includes the mobile number of both the person making and receiving the call, date, time and call duration, and low resolution location information (nearest cell tower).
[2] Note, most data protection laws apply to data from which an individual can be identified. Where it is possible for individuals to be identified from pseudonymous data, data protection laws will generally apply, but they also recognise that pseudonymisation is a valuable safeguard.

Mobile Operator Data in order help them to contain, delay or research the spread of the virus or to mitigate its impact on public health.

'Researchers' includes academic institutions that seek to access to the Mobile Operator Data acquired by the Governments or Agencies.

The GSMA COVID-19 Privacy Guidelines

The GSMA recommends the adoption of the following approaches for MNOs when considering requests for access to Mobile Operator Data in response to the spread of COVID-19:

Compliance with Law and Consideration of Ethics

- Comply with all applicable legal obligations and licence conditions
- Take proactive steps to implement privacy best practices such as the GSMA Mobile Privacy Principles[3] and consider the ethical implications of lawful sharing of Mobile Operator Data for the purposes of helping Governments or Agencies to contain, delay or research the spread of the virus or to mitigate its impact on public health
- Engage with Governments or Agencies and, where appropriate courts, to seek clarity when the legal basis for a request is unclear or uncertain or where additional emergency powers may be required to support a request

Sharing of Insights or Aggregated Non-Identifiable Data with Governments or Agencies typically falls outside the scope of general data protection laws to the extent that they are truly anonymous. Where data protection laws do apply to the use of Aggregated Non-Identifiable Data, it is typically permissible on grounds of being in the public interest, though MNOs will, of course, need to review and conform to local legal requirements.

In exceptional cases, Governments or Agencies could request Metadata relating to specific individuals, for example, to identify people who may have been in contact with confirmed cases, or to inform people if they have entered an affected area. This data should only be shared based on a valid legal ground for processing such as, depending on local law, obtaining the valid consent of the individual, acting in the individual's vital interests in an emergency, or pursuant to a specific law requiring the sharing of the data. Such a specific law should be necessary for the purpose of public security, and absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised privacy standards, human rights and other relevant laws.

Transparency

- Be transparent with the public about the sharing of Mobile Operator Data with Governments or Agencies, unless prohibited by law

3 GSMA Report: Mobile Privacy Principles Promoting consumer privacy in the mobile ecosystem

- Help Governments or Agencies to counter misinformation and raise awareness of data sharing to help combat COVID-19

Transparency is key to maintaining trust and preventing the circulation of unfounded rumours. It is vital that MNOs as well as Governments or Agencies are open with the public about the extent and nature of data sharing in the COVID-19 context.

Insights and Aggregated Non-Identifiable Data

- Prohibit re-identification of individuals from Insights and Aggregated Non-Identifiable Data within their respective organisations
- Perform the conversion of Metadata into Insights or Aggregated Non-Identifiable Data prior to sharing them with Governments or Agencies, and in order to avoid sharing the underlying data

The process of turning Metadata into Aggregated Non-Identifiable Data for policymakers should be carried out by the MNOs before these are submitted to Governments or Agencies in order to reduce the amount and sensitivity of data shared with Governments or Agencies.

When performing de-identification, whether via aggregation or other techniques, MNOS should assess the risk of re-identification, specifically relating to the external environment and the other available COVID-19 data sets. A privacy impact assessment should also be undertaken when de-identification is performed.

The format in which Insights or Aggregated Non-Identifiable Data are requested by Governments varies from country to country, making it harder to draw useful comparisons. MNOs can work with Governments and Agencies to improve their understanding of what is possible, to minimize information demanded and shared, and to work towards aligning their requests in the future, keeping in mind differences in the regulatory landscape and other relevant factors.

Metadata

- Only share Metadata with Governments or Agencies where it is lawful to do so, for example, in many jurisdictions, if it is in the individual's vital interests, or on the basis of valid consent, or a law specifically requires it. Such a law should be absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised privacy standards, human rights and other relevant laws

In exceptional cases, some Governments or Agencies could request Metadata relating to one or more individuals. A legal request of this type can be in the best interests of the individuals concerned including, for example, when identifying contacts of known COVID-19 cases or warning people that they may have entered or are entering an affected area.

General data protection laws like the European Union's GDPR typically allow personal data to be processed if it is in the vital interests of the individual or where valid consent has been given. However, whether it is lawful in a particular case will depend on the precise circumstances and legal jurisdiction.

Some laws and mobile licence conditions that are aimed at electronic communications data providers prohibit the use of Metadata for such purposes unless consent has been provided or unless it is permitted by a law passed specifically for the purpose of protecting public security.

Assurances from Governments or Agencies

- While, in all cases, data should not be shared except as consistent with law, MNOs should, as appropriate, seek assurances from the Governments or Agencies that they will:

Lawful and fair

Confirm that the use of the Metadata or Aggregated Non-Identifiable Data is lawful and fair regarding any individuals concerned, taking all circumstances and potential impacts into account. To the extent the request is based on a specific law in the interests of public security, that such laws are necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised privacy standards, human rights and other relevant laws.

Governments and Agencies are urged to seek the opinion of the data protection supervisory authority and/or national telecommunications regulator in the relevant country and to share these opinions with MNOs.

Additionally, Governments or Agencies should provide appropriate limitations of liability or indemnify MNOs against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data.

Transparency

Be as transparent as possible with the public about the use of Mobile Operator Data and the applicable legal framework.

Purpose Limitation

Clearly describe the purpose for which the Metadata or Aggregated Non-Identifiable Data is being shared and prevent it from being re-used for any alternative purpose and, in particular, purposes not related to combatting the spread of COVID-19. In the event that a Government or Agency will allow Researchers to access the Aggregated Non-Identifiable Data, it should vet, monitor and, if necessary, block any proposed research topics that are not in line with the original purpose.

Prohibition of Re-identification

Enforce a strict rule prohibiting the re-identification of Metadata or Aggregated Non-Identifiable Data by staff or Researchers except as permitted by law and with notice to the identified individuals.

Security

Have appropriate technological and organisational measures in place to secure all Mobile Operator Data when 'at rest' as well as 'in transit'. This includes appropriate access and authorisation protocols.

Data Privacy Impact Assessment

Conduct a data privacy impact assessment in respect of any Metadata or Aggregated Non-Identifiable Data received.

Avoid Discrimination and Respect Fundamental Rights

Respect principles of equal protection under law, and not to use Mobile Operator Data or analytical insights to discriminate improperly against individuals or groups, or to violate fundamental rights.

Researchers

Vet Researchers and the scope of their research projects appropriately and bind them to an equivalent standard of adherence to these guidelines. This should include monitoring their access and requiring deletion of any Mobile Operator Data on termination.

Retention

Delete any Mobile Operator Data after a defined period or once it is no longer needed for the agreed health-related purpose.

Accountability

Provide evidence that they have acted in accordance with the assurances given. Establish an independent oversight board to monitor adherence to these principles.

These materials below form part of a broader array of GSMA privacy resources and initiatives, which are described in detail in the following links:

- GSMA Mobile Privacy and Big Data Analytics
- GSMA Report: Safety, privacy and security across the mobile ecosystem
- GSMA Report: Consumer research insights and considerations for policymakers
- GSMA Report: Mobile Privacy Principles Promoting consumer privacy in the mobile ecosystem
- GSMA Report: Privacy Design Guidelines for Mobile Application Development
- GSMA Mobile Policy Handbook

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com