COVID-19 Privacy Principles

The COVID-19 pandemic illustrates both how critical data can be in addressing societal issues and the importance of safeguarding the privacy and security of that data. As organizations worldwide consider how to collect and use personal data to combat COVID-19, BSA offers 11 principles that may serve as guardrails to help companies and organizations address the privacy and security of COVID-related data.

Consider Using Data That Does Not Identify Individuals

Organizations can draw important information from aggregated, anonymous, and de-identified information. When possible, organizations should use such data rather than data that identifies an individual. For example, researchers and public health authorities can use aggregated location data to understand the effectiveness of social distancing measures, forecast how the virus may spread over time, and identify ways to better allocate testing and medical resources, without needing data that is associated with a specific individual.

Collect a Minimum Amount of Data

When an organization does need to collect an individual's personal data for COVID-related purposes, it should minimize the amount of data collected. In deciding what data to collect, organizations should also consider data quality, and recognize that different types of data are fit for different purposes by different actors. Organizations should use data that is relevant and effective for their purpose. Similarly, organizations should minimize their access to and sharing of personal data, consistent with the purpose of collecting that data.

Adopt Time Limits

Organizations should delete or destroy data when it is no longer relevant for the purpose it was collected – and ensure that data collected for COVID-19 purposes is not retained for a future unrelated or unauthorized purpose. This can be done by adopting responsible data destruction and data retention practices and assessing the continued need for COVID-related programs at regular intervals.

Be Transparent – and Tell Individuals Why Their Data Is Collected

Organizations should embrace the principles of transparency and purpose specification by telling an individual why her personal data is collected and using the data consistent with that explanation. Organizations that want to use data in other ways should obtain affirmative express consent to do so – and should support voluntary uses of data. For example, if a mobile application collects health information from users in order to give that information to public health officials combatting COVID-19, the mobile application should only use data for that purpose.

Adopt Strong Security Practices

Organizations should employ reasonable and appropriate security measures designed to prevent unauthorized access, destruction, use, modification, and disclosure of personal data. Those measures should reflect the volume and sensitivity of the data; the size, nature and complexity of the business holding the data; and the cost of available tools. For example, sensitive information like health data should be protected by strong data security measures.

Provide Heightened Protections for Sensitive Data

Certain types of personal data, like medical information and precise geolocation information may be particularly sensitive and thus should be subject to heightened safeguards, including requiring consent before processing. Organizations should also ensure that processing respects existing privacy and data protection laws, which may create different safeguards for different types of data, including employee data, financial data, and health data.

Assess Privacy Risks

Organizations should consider conducting privacy impact assessments for activities that are likely to result in high privacy risks. These assessments enable organizations to identify privacy risks that may arise from their activities and identify ways to mitigate those risks. For example, under the EU General Data Protection Regulation ("GDPR") organizations that determine the purposes and means of processing data must conduct data protection impact assessments for activities "likely to result in a high risk to the rights and freedoms of natural persons." In the context of COVID-19, these assessments can be helpful tools for organizations to identify and mitigate privacy issues that may result from collecting personal data.

Make a Maintenance Plan

Organizations should ensure that COVID-related technologies are regularly maintained over the course of their deployment. In particular, technologies should be capable of adapting to new information that can help improve a system's accuracy and security.

Embrace Privacy-Enhancing Technologies

Organizations should encourage the use and advancement of privacy enhancing technologies like differential privacy, federated learning, and homomorphic encryption. These technologies can help to analyze data in privacy-protective ways, including by enabling the use of machine learning techniques on data while it remains encrypted, or increasing privacy protection of a dataset by adding "noise" to the data that makes identifying a particular data subject more difficult.

Address Privacy and Security Through the Data Ecosystem

Many organizations will use technology developed by service providers to analyze data relevant to COVID-19, and may coordinate with other organizations in joint efforts to combat the disease. In doing so, those organizations should maintain responsibility for that data throughout its lifecycle and ensure that data processed on their behalf is subject to appropriate privacy and security safeguards. For example, organizations should ensure that service providers only process data consistent with their instructions, and adopt appropriate measures to protect the security of data they handle.

Do Not Discriminate

Organizations should support inclusive uses of data and should not use data in a manner that creates unfair or unlawful discrimination. For example, organizations should incorporate accessibility standards into COVID-related products and support their use in multiple languages when possible. Organizations should also recognize that different populations may face different challenges in addressing health issues like COVID-19, and should consider involving advocates, experts, and representatives of affected populations as they develop new products and services.