Business Roundtable

Protect Privacy of Personal COVID-19 Data

Mitigating the spread of COVID-19 and preventing future outbreaks will require public health authorities to identify, test and isolate individuals who may have been exposed to the virus. To achieve this goal, states should significantly scale up their contact tracing capacity, utilizing both technology-enabled and manual tracing.

Merging digital tools with traditional manual contact tracing methods will give federal, state and local public health authorities the ability to monitor and predict the virus's spread and to respond by directing resources where they are needed most.

Contact tracing systems may require the collection and utilization of personal information (e.g., health, location and proximity information) and should, therefore, adhere to principles of transparency, choice, minimization of personal data and nondiscrimination. A robust contact tracing system also should integrate with broader, national tracking (i.e., syndromic surveillance) systems to aid public health strategies to slow the virus spread.

Federal leadership is needed to establish a consistent, nationwide approach to virus monitoring and to ensure that any use of technology to trace and track the spread of the virus is effective, accurate, and deployed in a manner that protects individual privacy.

Business Roundtable calls on Congress to put in place uniform privacy and security safeguards for COVID-19 data that adhere to the following recommendations:

I. Sensitivity and Context

Privacy protection should be based on and vary with the sensitivity of collected data and the context in which the data are used. In the context of COVID-19, public health needs should be advanced while also adhering to privacy-protective controls such as limited use based on the sensitivity of the data. For example, personal data collected through contact tracing should be used only for public health purposes related to COVID-19 protection or treatment, but not for unrelated purposes.

II. Privacy Practices

In developing virus monitoring systems, developers should promote uses of data in de-identified or aggregate form, whenever possible. Data collection and usage should be tailored to the goals and objectives for preventing the spread of COVID-19. Public health authorities and developers of these systems should ask first whether objectives can be accomplished using aggregate, anonymized data or robustly de-identified data.

If identifiable, sensitive data must be used, such systems should:

1. Give preference to approaches that offer individuals choice and control appropriate to the context in question over the collection, use and/or sharing of their data. In the particular context of the workplace, companies should be permitted to require employees to participate in the use of screening, tracing and tracking for the sole purpose of preventing the spread of COVID-19 in the workplace in accordance with guidance from relevant public health authorities.

2. Be transparent about uses of the data and ensure there are both clear purpose specifications and reasonable use and retention limitations tied to avoiding spread of COVID-19. These limitations are particularly important for use of the data by government entities or by private sector entities for health insurance screening purposes.

3. Impose restrictions on any secondary use of information that is not reasonably related to the primary use or would not be reasonably anticipated.

4. Ensure that checks are in place to avoid unintended discriminatory uses of information.

5. Employ appropriate technical and organizational measures designed to safeguard the security and confidentiality of personally identifiable data. The data should also be protected cryptographically both at rest and in transit.

6. Ensure deletion of data after it is no longer needed.

III. Consistency, Uniformity and Liability

Congress should ensure that a uniform set of robust and consistent privacy and security protections for consumers are in place across states and local jurisdictions. Additionally, federal guidance for companies is necessary to provide clarity and consistency on the privacy of employee data. Companies that adhere to these guidelines or to legislatively-adopted safeguards should be protected from liability.