Data Privacy Considerations for Coronavirus Data Tools

Aaron J. Burstein, Alysa Z. Hutnik

March 28, 2020

Data is helping governments, researchers, and companies across the world track the spread of the novel coronavirus, monitor cases and outcomes of COVID-19, and devise ways to halt the virus's spread. As part of these efforts, raw data, software tools, data visualizations, and other efforts are providing the public and policymakers with insights into the growth of the pandemic.

Personal information — some of which may be highly sensitive — is key to many of these efforts. Although some regulators in the U.S. and abroad have made it clear that privacy laws and the exercise of enforcement discretion provide leeway to process personal information in connection with COVID-19, they have also made it clear that privacy laws continue to apply. Federal Trade Commission (FTC) Chairman Joe Simons advises that the FTC will take companies' "good faith efforts" to provide needed goods and services into account in its enforcement decisions but will not tolerate "*deceiving consumers, using tactics that violate well-established consumer protections, or taking unfair advantage of these uniquely challenging times*." And, with many eyes on the California Attorney General's Office in light of recent requests to delay enforcement of the California Consumer Privacy Act (CCPA), an advisor to Attorney General Xavier Becerra was quoted as stating: "*We're all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency*."

Devoting some thought to privacy issues at the front end of COVID-19 projects will help to provide appropriate protections for individuals and address complications that could arise further down the road. This post identifies some of the key privacy considerations for contributors to and users of COVID-19 resources.

1. Is Personal Information Involved?

Definitions of "personal information" and "personal data" under privacy laws such as the CCPA and the EU's General Data Protection Regulation (GDPR) are broad. Under the CCPA, for example, any information that is "reasonably capable of being associate with, or could reasonably be linked" with an individual, device, or household is "personal information." This definition specifically includes "geolocation data." Although some data sources provide COVID-19-related information at coarse levels of granularity, e.g., county, state, or national level, the broad definition of "personal information" under the CCPA, GDPR, and other privacy laws makes it worth taking a close look at geographic and other types of information to determine whether the data at issue in fact reasonably qualifies as "personal information," or if it is sufficiently anonymized to meet privacy definitions of de-identified and/or aggregate data. CCPA, HIPAA, and other privacy laws provide examples of what safeguards are expected to reasonably treat data as anonymized, and employing such standards can help avoid unnecessary privacy mishaps despite well-intentioned efforts.

2. What Level(s) of Transparency Are Appropriate About the Data Practices?

Although some COVID-19 tools may be exempt from statutory requirements to publish a privacy policy (e.g., the provider of the tool is not a "business" under the CCPA), there are still reasons for providers to explain what data they collect and how they plan to use and disclose the data:

- Disclosures help individuals to reach informed decisions about whether they want to provide their data, e.g., by downloading an app and allowing it to collect their location and other information. If business practices and consumer expectations are not reasonably aligned around the data practices, the failure to provide an appropriate privacy notice could be deemed an unfair or deceptive practice, inviting the scrutiny of the FTC or State Attorneys General.
- Developing a privacy policy (or other disclosure) can help provide internal clarification on what types of personal information (or not) an app or service needs and collects. A granular understanding of such data practices can help providers to identify and mitigate privacy and data security risks associated with such data practices.
- Developing a disclosure about a provider's data collection and usage can help clarify the decision-making structure among multiple stakeholders so that the group is better equipped to handle data governance decisions over the lifecycle of a project.

3. How to Address Government Requests/Demands for Personal Information?

Although much remains to be seen in how federal, state, and local governments will use personal information (if at all) to develop and implement strategies to slow the spread of coronavirus, it is not unreasonable to expect that government agencies will seek information from providers of COVID-19-related tools. The extent to which a provider can voluntarily provide information to the government — as well as the procedures that the government must follow to compel the production of information (and maintain the confidentiality of it in personally identifiable form) — depends on several factors, including what kind of information is at issue and how it was collected. Becoming familiar with the rules that apply to voluntary and compelled disclosures, and safeguards to help prevent such data from being subject to broad freedom of information laws, before a request arrives can help save valuable time down the road. In many of these scenarios, for example, aggregate or pseudonymous data may be sufficient.

4. What Considerations Are There for Licensing COVID-19-Related Personal Information?

Finally, any licensing of personal information in connection with COVID-19 tools deserves careful consideration, particularly if the CCPA applies. The CCPA imposes notice and opt-out requirements on entities that "sell" personal information. "Sell" is defined to include disseminating, disclosing, or otherwise "making available" personal information to for-profit third parties in exchange for "monetary or other valuable consideration." Several types of open source licenses require users to accept certain restrictions on their use and/or redistribution of licensed data or software. For example, the Creative Commons Attribution-NonCommercial 4.0 International license requires licensees to agree (among other conditions) not to use licensed content for commercial purposes. Obtaining this promise in exchange for personal information could constitute "valuable consideration" and give rise to a "sale" under the CCPA. In addition, while not a "sale," sharing personal information with a government authority would qualify as a disclosure under CCPA and would need to be accurately disclosed in the privacy policy.

Neither the California Attorney General nor the courts have interpreted the CCPA in the context of

open source licenses. Until more authoritative guidance becomes available, it makes sense to think through the potential obligations and other consequences of applying and accepting specific license terms to COVID-19-related personal information.

Bottom line: Personal information has a key role to play in shaping responses to the novel coronavirus. Privacy laws remain applicable to this information. Applying privacy considerations to COVID-19 related practices involving data collection, sharing, and analysis will help mitigate unnecessary harms to consumers, aside from those presented by the virus itself.

For other helpful information during this pandemic, visit our COVID-19 Resource Center.