Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

www.informationpolicycentre.com

Covid-19 Meets Privacy: A Case Study for Accountability

April 2020

Bojana Bellamy, President

In the pressing global fight against Covid-19, technological and AI solutions, involving massive tracking and data analytics, have brought into sharp focus public concern over our fundamental right to privacy. Some have even asked whether privacy will be the victim of Covid-19. And, some have pointed out that our fundamental right to life must trump our right to privacy.

However, most of us want and expect both. Most of us agree that data driven analysis and decisions, as well as data sharing among industry and governments, are indispensable in fighting Covid-19 and future pandemics—whether to anticipate the virus' spread and peak; to test new medications or forecast the need for hospitals, medical staff and equipment; to understand people's social interactions and likelihood of contamination; to verify that quarantine and social distancing measures are observed; or to enable those who have recovered from the virus to resume their work, life and other freedoms for the benefit of us all. And, we also agree that privacy is foundational to our democracies and must be protected now and in the post-Covid world. So, how can we have both—socially responsible collective action and privacy? The answers lie in organizational accountability.

Organizational accountability is an emerging concept in data protection and privacy regimes globally. It requires companies and the public sector to implement effective privacy and data management programs, measures, processes and tools and be able to demonstrate these to regulators, shareholders, business partners, and the public. It complements compliance with existing privacy laws, which may vary from country to country, and operationalizes applicable legal requirements. Accountability also goes beyond compliance and creates openness around decision-making processes for data use and sharing, thereby generating public trust.

This concept has been increasingly embraced by industry and public sector bodies around the world. Organizations have been appointing Chief Privacy Officers; establishing internal governance and oversight procedures; carrying out privacy impact assessments that balance risks to individuals and benefits of data uses; delivering user-centric transparency; training their staff about data privacy and ethics; imposing restrictions on service providers, business and government partners when using their data; implementing security measures and technologies; responding to complaints and individuals exercising their rights to know about data uses or delete data. And yes, they have also had to deal in an accountable and cooperative manner with regulators when things went wrong and they suffered security breaches. These accountability-based privacy programs deliver robust controls and protections for individuals and their data, while also enabling responsible data use and sharing, which is so essential for the growth of our digital society and economy. All industry sectors, from high tech to healthcare and telecom, are looking to organizational accountability as the mechanism to bridge the dual imperatives of privacy and innovative data use.

The fight against Covid-19 is a perfect case study for how accountability can enable both of these goals. Organizational accountability empowers organizations to react quickly and robustly at a time of crisis without sacrificing privacy protections, or the ability to do what is necessary and right for our collective wellbeing. When accountability measures are properly implemented, communicated and enforced, there is no better way to address not only legal privacy obligations, but also societal skepticism, distrust, and fear of unbounded surveillance and abusive data practices. This is especially true where speed is of the essence, frameworks for responsible data sharing have not yet been developed, the need for clear and practical controls is mounting and regulators are scrambling to provide their own views on using data in the context of pandemics.

So, what are the basic accountability measures that organizations of all types, including companies, governments, research and academic institutions, can agree on and implement immediately to address data privacy concerns and enable responsible collection, use and sharing of personal data in the fight against Covid-19?

1| Clearly defined and documented purposes of data use

Each proposed project must define clear objectives to set the boundaries of what can and should be done with the data and for what purposes. The proposed data purposes should be supported by evidence that data use actually addresses a particular need.

2| Proportionality test

The amount, manner and duration of data processing must be relevant, necessary and proportionate to the desired objectives. The organizations must be able to answer and document

the following considerations: (1) Can we achieve the same objective with less data, or by using aggregated or fully anonymized data that does not identify any individuals? (2) Is the data processing we are proposing a proportionate response for the goal we are trying to achieve? And if not, what do we need to change and do to make it proportionate?

3| Privacy impact assessment

Organizations must assess the level of risk of data use or sharing and the potential impact on rights and freedoms of individuals for each project. Risk may be higher if a project involves sharing of health or geolocation data. In that case, what specific mitigation measures should be put in place to address this heightened risk? The assessments must also include an assessment of identified risks against benefits of data use and, especially, the reticence risk. There may be great costs for not using data-driven technology in crisis contexts, even to our other fundamental rights, including life, health and movement.

4| Transparency to individuals

Individuals whose data is being collected, shared and used must be given user-friendly information about the project and the uses of their data. This can also include information about controls implemented to address any data privacy risks and anything else that would build their trust in and acceptance of the project, such as where to address questions and requests to exercise data protection rights.

5| Robust security

Security is one of the cornerstones of data privacy. It must be maximized in the Covid-19 context to avoid unauthorized access to sensitive data, tampering with machine learning algorithms that may be used to forecast the need for hospitals, medical staff and equipment, make diagnoses or anticipate the hacking of critical IT systems.

6| Storage and use limitation

Data processing undertaken in the Covid-19 context to predict virus peak levels or to understand people's interaction and likelihood of contamination, must be conducted under clearly limited time frames. Once the purpose of processing is fulfilled, data should not be stored and used any more for another new objective that is unrelated to the original purpose.

7| Roles, responsibilities and training

All staff, contractors and third parties working on the project must be clear on their roles and responsibilities in delivering accountability measures and ensuring privacy protection. Organizations must provide everybody with role based training and set expectations for acceptable behaviors.

8| Data sharing agreements and protocols

Organizations sharing information must define their respective rights and obligations and specific controls relating to data use in a legally binding instrument. The protocols must include oversight and review mechanisms to escalate any issues and ensure all parties act in accordance with the agreement.

9| Trust, but verify

Organizations must conduct assessments and audits, and verify that they are implementing all the requirements, controls and accountability measures specified in the project and any third party agreements.

10| Internal oversight and external validation

The more complex and high risk the data use/sharing project is, the greater the need to ensure internal top management and Chief Privacy Officer oversight and clear accountability of leadership in the organizations. This may also involve some

forms of external validation, with external ethics or data advisory councils, or data review boards where these are already in place.

11| Regulatory engagement and validation

Organizations must be prepared to demonstrate accountability measures and seek feedback on the project from data privacy regulators. This can be either in the planning phases, or post-facto, on request, or in the case of a complaint or another issue. Constructive engagement between organizations and regulators is especially crucial in the Covid-19 climate where new and unforeseen uses of data are becoming essential for protecting the public. By discussing and navigating relevant challenges together, organizations and regulators can achieve necessary and quick outcomes that comply with applicable requirements and generate public trust. Such efforts will also set data privacy regulators up to establish a unified approach to regulating data in emergencies for the future.

12| Privacy-by-design through technical measures

Organizations must consider how technical measures can help ensure privacy-by-design in new data projects. For example, differential privacy, anonymization and federated learning can be useful techniques when deploying AI and machine learning applications.

By implementing the above measures, both the public and private sectors will ensure digital responsibility, enabling data innovation and delivering effective privacy protection. Public authorities, in particular, have a leading role to play in applying accountable practices in the Covid-19 context. Data often travels between the public and private sectors and it is critical that governments refrain from any practice that could jeopardize trust in technology and the digital economy to help solve this crisis. When requesting access to or sharing of data from the private sector, governments must implement all appropriate accountability measures and protections we discuss above. In particular, their requests must be based on a statutory or other legally permissible requirement and their use of data strictly limited for the purpose of a specific Covid-19 initiative.

Individuals, industry, academics, public authorities and society at large—we are all engaged in the same battle against the coronavirus. Our key advantage over previous pandemics is technology and data, which have armed us with new and effective resources against the virus' destructive potential. We must use them to the fullest. In times of danger, individual privacy cannot trump our social responsibility towards others. Nor should the common good have to trump privacy. Accountability enables us to enjoy both and to have our privacy cake and eat it together.