LETTER TO THE EDITOR

Privacy, Equity, and Human Rights Challenges in Public Health Surveillance

RACHELE HENDRICKS-STURRUP AND SARA JORDAN

In the situation of a global pandemic, how can specific vulnerable groups be protected against privacy risks that are inherent to contact tracing? Over the last 19 months, this question has motivated intense discussion by bioethicists, health law and privacy scholars, technology companies, and governments. Some of the nuance of that discussion was captured within several pieces published in *Health and Human Rights Journal*, including but not limited to "Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis." These and other authors advocate for scrutiny of digital contact tracing technologies (DCTT) for two reasons: (1) the historic pattern whereby emergency public health or safety surveillance systems later became embedded as "permanent fixtures," sometimes to the detriment of basic access to essential public services, and (2) the trend of digital health surveillance tools as harbingers of unmanaged privacy, safety, and security risks.

The Future of Privacy Forum recently grappled with pandemic privacy and equity risk in our Privacy and Equity Principles and Framework for DCTT, solidifying the perspective that

> *contact tracing efforts to monitor the spread of communicable diseases in socially vulnerable groups can place those groups at risk of discrimination or ostracism at home or within their communities. Those populations may suffer the greatest, from a social and economic standpoint, and may be less likely to engage in any technology, including DCTT, that might disclose their private social affiliations and whereabouts.*

This framework argues that the protection of vulnerable persons in the midst of heightened risk requires (at least) the following commitments:

1. Be transparent about how data is used and shared.
2. Apply strong de-identification techniques and solutions.
3. Empower users through tiered opt-in/opt-out features and data minimization.
4. Acknowledge and address privacy, security, and nondiscrimination protection gaps.
5. Create equitable access to DCTT.
6. Acknowledge and address implicit bias within and across public and private settings.
7. Democratize data for public good while employing appropriate privacy safeguards.
8. Adopt privacy-by-design standards that make DCTT broadly accessible.

Rachele Hendricks-Sturrup, DHSc, MSc, MA, is a health scientist, research director of real-world evidence at the Duke-Margolis Center for Health Policy, Washington, DC, USA, and former health policy counsel and lead at the Future of Privacy Forum, Washington, DC, USA.

Sara Jordan, PhD, is a bioethicist, technologist, and senior researcher at the Future of Privacy Forum, Washington, DC, USA.

Our framework identifies five real-world case scenarios where manual or digital data collection or use has conflicted with the notion of privacy as a basic human right. For instance, we found in two cases that principles 4, 6, and 8 above were not implemented by the DCTT developers or users, thus creating situations where information gained from DCTT was used to target vulnerable groups. With respect to the future, we found that without careful consideration of social vulnerabilities, such as discrimination or ostracism, DCTT implementation will be less effective when used among populations who fear disclosure of their already stigmatized private lives.

As the COVID-19 pandemic continues, new technological solutions will test the real-world application of these principles. We hope that like-minded venues, including *Health and Human Rights Journal* authors and readers, can continue to ask and answer these challenging questions with fundamental human rights, privacy, and public health in mind.