Community Oversight of Surveillance - D.C.

June 2, 2020

Executive Office of the Mayor
The Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, NW
Washington, DC 20004

Dear Mayor Muriel Bowser
Chairman Phil Mendelson,
Councilmember Charles Allen,
Councilmember Anita Bonds,
Councilmember Mary Cheh,
Councilmember Vincent C. Gray,
Councilmember David Grosso,
Councilmember Kenyan McDuffie,
Councilmember Brianne K. Nadeau,
Councilmember Elissa Silverman,
Councilmember Brandon T. Todd,
Councilmember Robert White, Jr., and
Councilmember Trayon White, Sr.,

Dear Mayor Bowser and DC Councilmembers:

We are a broad coalition of local and national stakeholders including civil rights and civil liberties organizations, grassroots organizing groups, service providers, and District residents who are working to bring transparency and community input to the District's use of surveillance technologies. As your offices and related agency departments work toward implementation and scaling up of contact tracing measures to assist the District's reopening, we urge you to engage the community and adopt policies that respect the privacy, civil rights, and civil liberties of your constituents, and to then be transparent about those policies.

Contact tracing is an important tool for governments to use in helping curb the spread of COVID-19. However, in the course of contact tracing interviews, community members are asked to disclose sensitive information reflecting their location history and their associations. We write to secure assurances that information collected for this purpose is appropriately limited to public health authorities and will be deleted once no longer needed, and that compliance with contact tracing, even as it is strongly encouraged, does not under any circumstances result in punitive measures being taken against non-compliant individuals.

In addition, we are aware that other jurisdictions are seeking to use technology to supplement manual contact tracing. Should the District's public health authorities deem it necessary and effective to use digital tools—such as a Bluetooth-enabled exposure notification app—to assist in its contact tracing efforts, those tools should be designed in a privacy-protective and inclusive manner. Because you may be considering adopting such a tool, or may be approached by app developers, we raise the following concerns with you in an effort to improve the efficacy of any contact tracing the District pursues and ensure that the rights of District residents are protected.

Just as the District should deploy any public health resources like manual contact tracing in an inclusive manner, any digital tools under consideration must be built and deployed with an eye toward the inequities laid bare in the spread of coronavirus, as well as the inequities inherent in any technology-driven solution. Smartphones are a prerequisite for participation in any digital exposure notification app. Though 81% of Americans now own smartphones, the populations that are without smartphones are largely lower income and elder Americans[1]—the same populations that have been at highest risk during the spread of coronavirus. Further, in the District, the disparate racial impact of coronavirus has been particularly stark: though Black residents make up less than half the population, they have made up 76% of COVID-19 deaths, and though Hispanic and Latino individuals only make up around 11% of the population, they make up about 25% of all cases to date.[2]

The success of any digital exposure notification tool depends upon high participation; epidemiologists have estimated that around 60% of the population will need to participate for an app to be effective.[3] Accordingly, residents must trust that the relevant app will not be used to track them, will not lead to law-enforcement involvement, and will not render them less safe. It

---

[1] Pew Research Center, Mobile Fact Sheet. June 12, 2019. https://www.pewresearch.org/internet/fact-sheet/mobile/

[2] District of Columbia Office of the Mayor, DC COVID-19 Data published May 26, 2020. https://coronavirus.dc.gov/page/coronavirus-data; U.S. Census Bureau, QuickFacts: District of Columbia, accessed May 26, 2020. https://www.census.gov/quickfacts/fact/table/DC#

[3] Dave, Paresh, "Explainer: How smartphone apps can help 'contact trace' the new coronavirus." *Reuters.* April 14, 2020. https://www.reuters.com/article/us-health-coronavirus-tracing-apps-expla/explainer-how-smartphone-apps-can-help-contact-trace-the-new-coronavirus-idUSKCN21W2I8

is therefore critical that the District be guided by strong privacy safeguards, which can form the basis for strong public trust in, and support of, a government's deployment of any new technology. Further, for manual tracing efforts and digital tools alike, where there is tension between these goals, we urge the District to err on the side of public trust.

As the District develops its contact tracing program, we hope it will be guided by the following principles:

1. Led by public health officials

The development and deployment of any contact tracing strategy must be guided by input from infectious disease experts who can properly identify infection risk with an understanding of transmission methods and community interactions. Any contact tracing strategy must also be part of a larger structure of widespread, affordable, and prompt testing deployed alongside adequately funded medical and social interventions, including financial and social supports for self-isolation. With respect to contact tracing tools, and digital tools in particular, public health officials, in consultation with technical and other experts, must evaluate the tool's effectiveness and confirm that it will be effective in helping to stem the spread of coronavirus.

2. Use Limitations, Data Protection, & Data Minimization

Any data collected as part of the District's contract tracing efforts should not be used for purposes other than public health. Data should not be used for secondary purposes including commercial advertising use and any punitive or law enforcement purposes. Under no circumstances should the Metropolitan Police Department (MPD) or any other law enforcement entity in the District have access to data collected via contact tracing efforts, including but not limited to the names and addresses of those who have contracted coronavirus. Sharing data with law enforcement would not only have a chilling effect on voluntary participation in contact tracing efforts and COVID-19 testing, but would also increase the risk of misuse of data by law enforcement to further racially discriminatory and harmful policing practices in the District.

Policies must therefore be in place to ensure that only necessary information is collected, and to prohibit any data sharing with any person, agency, or private entity outside of public health authorities.

3. Transparency

The District must be fully transparent about its contact tracing strategy, including by providing the public with specific information about the tools it plans to use, from where it acquired them and at what cost, how it plans to use them, and what measures it will have in place to protect the

personal data collected. The government must also be fully transparent about what types of data it is acquiring, from where, how it will use that data, and how long and where the data will be stored.

The District should also be transparent in sharing the impact of its contact tracing efforts on the spread of infection rates. Seeing that a tool has marked and measurable effects on the spread of infection will increase public confidence in its use, which in turn will lead to increased utilization. This can be communicated through disclosure of metrics such as the number of reported exposures and self-isolations, in addition to the COVID-related data the District currently publishes.

4. Oversight and Accountability

Not only should there be safeguards in place to detect and prevent unauthorized sharing of or access to user data, but there should be oversight and accountability for all actors involved, including any app providers, and the government authorities. There should be clear, enforceable penalties for violations, and the Attorney General of D.C. should be empowered to enforce them. Further, any app the District uses should be subject to regular independent audits that are made public and should be released as open source.

5. Limited to the COVID-19 crisis

Policies must be in place to ensure the District's contact tracing program does not outlive the effort against COVID-19. We caution against the deployment of any contact tracing strategy or tool that is intended for application in all future pandemics. A contact-tracing strategy should only last so long as it is effective, or as long as the current pandemic lasts, whichever is earlier. The District's strategy should include clear markers for when to stop operations, and a sunset plan for the disposal of collected data once contact tracing of COVID-19 is no longer necessary.

Specifically with respect to any digital tool that is used to supplement the efforts of manual contact tracing, we strongly urge following these additional principles:

1. Voluntary Nature

As part of the District government's commitment to transparency, its contact tracing system must provide residents with sufficient information and autonomy to meaningfully decide whether to participate in an exposure notification app and how to respond to an alert of possible exposure. The decision to use any relevant app should be voluntary and uncoerced. This extends to choices about whether to carry a mobile device, install an app,

disable or at least turn off an app during times of inactivity, upload a log of contacts, and select which medical providers will receive what data.

2. No Use of Location Data for Tracking

Digital exposure notification apps, and their data, should not be used for purposes of tracking individuals. Designs that center on proximity data (from Bluetooth technologies), rather than collecting and recording an individual's location data, are preferable both from an efficacy and privacy standpoint. These tools may help show whether two individuals have come into close enough contact to risk transmision of the virus, which is the information actually needed for contact tracing. Further, as compared with collecting actual location information, gathering only proximity data minimizes the risk of data being repurposed or used to re-identify individuals, and can therefore put community members at ease that they aren't under surveillance.

In the absence of strong privacy legislation from Congress, we urge the D.C. Council to consider passage of legislation that would codify the policies enumerated above in order to safeguard the privacy of District residents and allow for robust oversight and accountability.

Finally, and importantly, we urge you to engage the public before adopting a tool, and our coalition stands ready to serve as a resource on this matter. As you make decisions about the District's contact tracing strategy, we hope that you will be guided by the above principles and demonstrate the District government's commitment to transparency as well as the protection of residents' privacy and autonomy. Overall, strong privacy protections are critical to engendering public trust, which is vital to an effective fight against the pandemic. Thank you for your efforts and leadership through this difficult time, and we hope that we can continue to work together on this and other surveillance issues as they arise.

Sincerely,

Members of the Community Oversight of Surveillance-D.C. Coalition
and supporting organizations

CC: Director Laquandra S. Nesbitt, MD, PHD, D.C. Department of Health

---

ACLU of the District of Columbia

Center for Democracy & Technology

DC Open Government Coalition

HIPS

In the Public Interest

Justice For Muslims Collective

Kandoo

Lucy Parsons Labs

New America's Open Technology Institute

Showing Up for Racial Justice (SURJ) DC

Sisterhood of Salaam and Shalom DC-II Chapter

Stop Police Terror Project DC

Upturn