May 4, 2020

Governor Jay Inslee
Office of the Governor
PO Box 40002
Olympia, WA 98504-0002

Sent Via Email Only

RE: Technology-Assisted Contact Tracing & Exposure Notification Tools

Dear Governor Inslee,

On behalf of the ACLU of Washington, we thank you for your commitment and efforts to protect public health during the COVID-19 pandemic. As the Governor's office and state agencies consider different strategies to begin reopening the economy and getting people back to work, we write to lift up civil liberties concerns as they relate to the many technology-assisted contact-tracing (TACT) proposals that have been presented as potential solutions to the public health crisis.

We emphasize that on their own, technology-assisted contact tracing and exposure notification systems cannot stem the spread of COVID-19 and are only useful if those who learn of possible exposures to COVID-19 are able to get testing, counseling, and treatment, and to take measures such as self-isolation. These services must be widely available and affordable in order for TACT to be an effective tool.

As your office evaluates whether and how to use different technologies, we recommend considering the following basic principles to ensure that any TACT tool implementation protects both public health and civil liberties.[1] These principles are described in greater detail in this ACLU white paper.

(1) The tool should not displace non-technological, known, and effective public health measures such as testing, counseling, research, and treatment. Every TACT proposal is predicated on the availability of widespread, affordable, and prompt testing, and without such measures, deploying a TACT tool may actually divert resources from testing, which is perhaps the most vital public health measure.

(2) The tool must be voluntary at every step. A compulsory TACT tool may pose threats to people's fundamental rights to privacy and association, and may dissuade people from using it, decreasing the tool's effectiveness. Steps where users should be able to exercise choice include deciding whether to carry a phone with them at all times, install the tool on their phone, or disable the tool; whether and

[1] Many of these principles, including that the tool should be voluntary, privacy-preserving, and non-punitive, should also be considered in the context of traditional contact tracing.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

P.O. Box 2728
Seattle, WA 98111-2728
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

how to react to alerts indicating they have been exposed to the virus; which medical providers to engage with; and if diagnosed, whether to share their diagnosis or log of contacts. Furthermore, people's ability to work, shop for groceries, or access public benefits must not be conditioned upon usage of the tool.

(3) The tool must be non-punitive. The tool and the data collected by it must not be used for punitive measures including arrest, criminal prosecution, immigration enforcement, or quarantine enforcement. Any data must not be made available to state, local, or federal law enforcement. The effectiveness of TACT tools depends on widespread adoption, and widespread adoption requires public trust that the application will not be used to harm people.

(4) The tool must be non-discriminatory. The tool must account for and mitigate the risks of it being used to further exacerbate social inequities. For example, if expedited testing is granted to people for owning a device capable of running the tool, implementation of the tool may amplify existing disadvantages faced by poor and elderly communities, who are less likely to have a compatible mobile device or a device at all. These communities are already at an elevated risk of dying from COVID-19. The deployment of any tool should be coupled with efforts to identify populations likely to be misrepresented or excluded by the system and find solutions to ensure their needs do not go unmet.

(5) The tool must be rooted in science and built with the guidance of public health professionals. Key decisions such as how to measure when two phones have been close enough together to be medically relevant, or whether a verified diagnosis of COVID-19 would be required before proximity alerts would be sent must be made in tandem with public health professionals and infectious disease experts. If a key goal is to use the tool to prioritize delivery of scarce medical resources to those most at risk for infection and to avoid wasting medical resources on false alarms, such decisions must be made carefully with professionals who understand the characteristics of disease transmission and have experience in how to effectively prioritize medical care.

(6) The tool must have a measurable impact. Any deployment of the tool must be accompanied by a plan for measuring and publicly reporting its impact and effectiveness.

(7) The tool must be terminated if shown to lack effectiveness or when the public health crisis ends. Any tool designed to target a particular crisis must not last beyond the crisis and must be shut down if shown to lack effectiveness at targeting the crisis. The tool must have built-in measures to phase itself out and developers of the tool as well as the public must understand when to "declare victory" and cease

operations, when to terminate the tool due to lack of effective impact, how to shut down any central servers or authorities safely, and how to uninstall the tool or stop operation on people's devices.

(8) The tool must be privacy-preserving. The tool must not collect or transmit any data not strictly necessary for the specific public health function of stemming the pandemic. The tool should be designed to maximally preserve privacy through technical limitations on its ability to collect, store, and transmit data, and must not rely solely on policy guidelines to enforce that privacy is maintained. For example, developers should ensure that data collected remain local to devices controlled by the device's owner where possible. Further, any identifiers used by the system should not be able to be connected to other identifiers, including but not limited to phone numbers and IP addresses.

(9) The tool should minimize reliance on central authorities. The tool should avoid sending detailed information such as location history to central authorities under either government or private control. Sending data to central authorities leaves users little to no control over what happens to that data once it leaves their devices. Data that are warehoused in centralized databases are vulnerable to security compromises, subpoenas, and disclosure orders.

(10) The tool should be clear about which central authorities will receive user data, and for what purpose. It must make these decisions clear so that the public can know in whom they are placing their trust, and for what purpose.

(11) The tool should follow data minimization principles. The tool should keep data encrypted at rest (locally encrypted) where possible, schedule any data collected to be destroyed after the latest epidemiologically relevant date (e.g., a date based on the incubation period of the virus), and avoid sharing granular or detailed data that increase the risk of individuals being identified.

(12) The tool should not share data with uninvolved parties that have not been designated as necessary for a predefined public health purpose or to ensure the tool functions. There must be legal, procedural, and technical safeguards to prevent any uninvolved third parties such as law enforcement agencies from accessing any data stores as well as mechanisms to detect unauthorized access and penalties for doing so. For example, in addition to requiring that the tool is secure from data breaches, policymakers must prohibit private entities from using information collected by the tool for any commercial purpose, except for public health purposes explicitly authorized by public health officials.

(13) The tool must be narrowly tailored to target this specific health

crisis. The tool must specifically be designed to target COVID-19. A tool that aims to target all imaginable future pandemics would require gathering information that is not necessary to combat COVID-19. This would reduce trust in the system, diminishing the tool's effectiveness. Furthermore, overbroad information gathering would divert resources needed to make the most effective tool to counter this specific health crisis.

(14) The tool must be auditable and fixable. The tool must be transparent to review and improvement by the general public. Communities and users should be able to audit the tools themselves without relying on a single auditing scheme. One key step in creating a transparent tool is to make sure it exclusively uses open source components.

(15) The tool must be sustainably maintained. While the tool must have an exit strategy, it must also be actively maintained throughout the COVID-19 pandemic. The TACT system must be able to change and adapt to circumstances while it is deployed and must be supported by enough resources to make any necessary adaptations responsibly (e.g., by addressing problems discovered in the software or incorporating changes in our understanding of the disease and its social impacts). Funding and support should be available for resources including community liaisons, public health professionals, user interface and user experience ("UI/UX") designers, cryptographers, security researchers, software developers, and system administrators.

While adopting a technology-assisted contact-tracing tool may be useful in reopening Washington's economy, we urge you to consider the risks that poorly designed systems pose to both public health and our civil liberties. We recommend considering the basic principles outlined above when evaluating any TACT proposal. A TACT tool that fails to comply with the recommendations above could violate Washingtonians' right to privacy protected by Article I, Section 7 of the Washington Constitution and other laws.

Thank you for all the work you are doing to address this health crisis. We hope you consider the ACLU of Washington as a partner and resource in responding to this crisis.

Sincerely,

Michele Storms
Executive Director