May 15, 2020

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

*Sent by email only*

RE: Protect privacy as part of COVID-19 requirements for businesses to collect and retain customer information

Dear Governor Inslee,

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*

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 your office begins to issue COVID-19 rules for businesses to reopen, we write to request that safeguards for customer privacy be included in requirements[1] for businesses to collect and retain data about customers' contact information (telephone numbers and email addresses) and times of entry for the purpose of facilitating contact tracing. Methods which both protect privacy and promote public health are described below.

We emphasize that privacy-friendly and voluntary measures are often more beneficial to public health goals than mandatory measures or measures that make people fear the loss of their privacy and loss of the freedom to choose which businesses to enter or patronize without revealing their identity. While we respect that the recently issued customer logging requirements aim to improve the process of manual contact tracing, the mandatory collection of contact information from customers is an invasion of privacy. Tracking which businesses a person enters, and when and where individuals congregate together, will also have a substantial chilling effect on people's freedom of association and freedom of expression.

---

[1] **Restaurants & Taverns:** "Phase 2 Restaurant/Tavern Reopening COVID-19 Requirements," Washington State Governor's Office, May 11, 2020, https://www governor wa gov/sites/default/files/Phase%202%20Restaurant%20industry%20re-open%20proposal_FINAL pdf
**Car Washes:** "Phase 1 Car Wash Industry COVID-19 Requirements," Washington State Governor's Office, May 7, 2020, https://www governor wa gov/sites/default/files/COVID19%20Phase%20One%20Car%20Wash%20Requirements pdf
**Landscape Services and Outdoor Maintenance Industry:** "Phase 1 Landscape Services and Outdoor Maintenance Industry COVID-19 Requirements**,"** Washington State Governor's Office, May 8, 2020, https://www governor wa gov/sites/default/files/COVID19%20Phase%201%20Employee%20Safety%20and%20Health%20Landscaping pdf
**Pet Walking Industry:** "Phase 1 Pet Walking Industry COVID-19 Requirements," Washington State Governor's Office, May 8, 2020, https://www governor wa gov/sites/default/files/COVID19%20Phase%201%20Employee%20Safety%20and%20Health%20Pet%20Walking%20Guidance pdf
**Vehicle & Vessel Sales:** "Phase 1 Resuming Vehicle and Vessel Sales COVID-19 Requirements," Washington State Governor's Office, May 6, 2020, https://www governor wa gov/sites/default/files/Phase%201%20Resuming%20Vehicle%20%20Vessel%20Sales%20FINAL pdf

We have serious concerns with any plan that would require people to disclose their names and/or contact information and whereabouts without strict controls on the storage and accessibility of such information. Normally, judicial oversight or, at a minimum, informed consent would be required to allow others to access and use personally identifying information and related data about travel and association with others. Business logs cannot be susceptible to disclosure beyond the tightly limited purposes of contact tracing. Without appropriate safeguards, contact information can be disclosed to immigration agents, law enforcement, advertising companies, identity thieves, stalkers, and harassers. If providing contact information is mandatory, rather than voluntary, this may have the effect of excluding people from public accommodations for fear of nonconsensual data sharing and other forms of surveillance abuses.

Furthermore, even if the customer logging rules were voluntary rather than mandatory, we are concerned that the recently issued requirements do not address how businesses must protect customers' private information. The rules refer to businesses keeping logs, but do not specify exactly what information must or may be requested. The rules refer to the daily log "*including* telephone/email contact information" (emphasis supplied) but do not *exclude* the collection of other information. Moreover, it is unknown whether businesses will be collecting telephone numbers or email addresses or both, and whether personal or work contact information will be logged.

If people do not trust that their data are being protected or fear that their data will be stolen, sold, repurposed, or used for criminal or immigration enforcement purposes, they may be less likely to participate in measures that may be beneficial for public health. Some people may still choose to patronize in-person businesses but may provide inaccurate information to protect their privacy or refuse to provide information altogether.

Additionally, compulsory customer logging without strict policies to protect privacy and civil liberties may lead to law enforcement becoming involved in implementation of these requirements. This is of concern because public health experts have cautioned that a punitive approach to combating disease is less effective than relying on voluntary measures.[2] People should not be punished or otherwise disadvantaged for refusing to provide their contact information. Access to public accommodations, such as stores and restaurants, should not be conditioned on providing personal information or carrying identification. Punitive policies also raise racial equity concerns. Experience has shown that sanctions are almost invariably imposed disproportionately on people of color.

---

[2] George J Annas, Wendy K Mariner,
and Wendy E Parmet, "Pandemic Preparedness: The Need for a Public Health – Not a Law Enforcement/National Security – Approach," American Civil Liberties Union, January 14, 2008, https://www aclu org/sites/default/files/pdfs/privacy/pemic_report pdf

Given these concerns, we ask that the Governor's office incorporate the following recommendations into any current and future COVID-19 requirements issued for businesses to reopen.

**1. Ensure that any data collection policy is voluntary.** Customers must not be required to provide their information to businesses. To ensure any information provided is voluntary, customers must be told that they have a right to decline to provide their information, for what purposes any information collected will be used, and with whom their data will be shared.

**2. Ensure that any data collection policy is equitable and does not mandate showing identification**. A data collection policy must not require customers to show identification. Requiring people to show identification will exclude many people who do not have it—including immigrants, the poor, the elderly, and people of color—from access to important services. It would increase the potential that a person attempting to enter a business without identification could be stopped by law enforcment or arrested. The United States has never had a national identification card or any requirement that people carry identification with them everywhere they go, and we should not create such a requirement now.

**3. Ensure that any data collection policy is strictly limited to the predefined purpose of facilitating contact tracing to target COVID-19.** Public health officials and government actors must only use any customer logs created to faciliate contact tracing. There should be a prohibition on all access and uses other than for this predefined purpose.

**4. Ensure that customer data are protected and are not shared with parties that are not necessary to the contact tracing response.** Businesses that collect customer information and anyone authorized to use that information for contact tracing must be required to adopt safeguards to prevent any uninvolved third parties from accessing customer logs, and be subject to penalties for failing to do so. Businesses should limit the number of employees who have access to customer logs and use recommended security procedures to protect customer contact information.[3] Anyone who improperly accesses customer logs should likewise be subject to penalties. Law enforcement and prosecutors should not be able to seek customer logs for any criminal or immigration enforcement purposes.

**5. Ensure that there are transparency and auditing mechanisms for any data collection policy.** Officials should be transparent about how any data collection policy will be implemented and enforced. There should be independent auditing and oversight measures to ensure that any data collection policy is being implemented solely for predefined public health purposes, is effective at fulfilling that purpose, and is limited to the duration of the pandemic. The government should maintain documentation of any request made to obtain information from a customer log,

[3] "Protecting Personal Information: A Guide for Business," Federal Trade Commission, October 14, 2016, https://www ftc gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

including who made the request, whether information was disclosed, how such information was used, and whether such information was retained by the requester. Such documentation should be available to independent overseers, including relevant legislative oversight bodies.

**6. Ensure that data collected are not stored in a centralized or shared database.** Businesses themselves should be the entities to maintain customer logs and should only provide customer information to public health agencies when they receive an appropriate and documented request. Avoiding storing customer information in a shared database mitigates security threats and potential abuse by private or government actors. Ensuring that data storage is decentralized and easily separable is important (e.g., making sure that one store in a chain cannot access data from other stores in that chain). Additionally, businesses should be encouraged to use paper instead of electronic records, as paper customer logs are not easily aggregated and made centrally searchable, shareable, and subject to repurposing for non-public health purposes. Paper records are as effective as digital records for the purpose of maintaining customer logs; if a person who has tested positive for COVID-19 has visited a business, the relevant records can easily be obtained from a business maintaining a decentralized and paper customer log. Lastly, businesses should not be permitted to use ID scanners to collect customer data.

**7. Ensure that data collection is minimized.** Businesses should only ask to collect the minimum amount of information necessary to achieve a necessary and proportionate public health response. The requirements should specify exactly what information may be requested for the log, and collection of information beyond that should be prohibited. Names and exact times of entry should not be recorded, as collecting and retaining exact times of entry are not necessary for the public health purpose of notifying individuals who may have been exposed to the virus, but increase the likelihood that the customer logs may be repurposed by private and government entities outside of the COVID-19 context. Contact tracers would likely notify anyone who had visited a business on the date of the infected person's visit, because a person's time of entry into a business such as a restaurant, does not determine when they leave. Collecting date of visit can provide sufficient granularity for contact tracers.

**8. Ensure that data collected are destroyed after the minimum period of time necessary to retain the data for the purpose of conducting COVID-19 contact tracing.** Any policy should ensure that customer logs will be held no longer than needed for contact tracing, and destroyed regularly. Public health officials should advise policymakers on the period of time after which the data are no longer useful for contact tracing purposes, and businesses should be required to delete customer data after that period of time. Reasoning for any required retention period should be shared with the public.

**9. Ensure that any data collection policy is terminated if shown to lack effectiveness or is no longer necessary for the purpose of targeting COVID-19.** Any policy 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.

Government entities, businesses, and the public must understand when it is appropriate to terminate the policy and how to securely destroy any data collected.

In conclusion, while customer logging may be a useful measure to protect public health in the process of reopening Washington's economy, we urge you to consider the risks to both public health and civil liberties posed by unclear or overbroad data collection policies. We ask that your office incorporate the safeguards outlined above into any current and future COVID-19 requirements issued for businesses to reopen.

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

Sincerely,

Michele Storms
Executive Director