Comparison of Access Now's Data Protection Recommendations and the U.S. Senate Republican COVID-19 Consumer Data Protection Act	
Access Now recommendation	Does the bill meet the recommendation?
Purpose limitation and data minimization	😐The bill limits the types of data it applies to (Sec. 2(6)), the purposes for which data processing is allowed (Sec. 3(b)), and includes data minimization requirements (Sec. 3(g)). However, so-called "de-identified" data is largely exempt from the bill's protections. Such data can thus be used without restriction, leading to potential privacy invasions as de-identified data can often be re-identified. The data minimization requirements are similarly lax, as they allow collection of what is "reasonably" necessary, potentially broadening the types of data that can be collected.
Access limitation and data security: Access to health data shall be limited to those who need information to conduct treatment, research, and otherwise address the crisis. The information should be stored securely, in a separate database.	😐The bill merely requires companies to take "reasonable" steps to protect the data they collect, without any conditions on where and how data should be stored or who can access the data (Sec. 3(h)). More guidance is necessary, particularly given health data is private and personal.
Data retention and future research: Data processed in response to the crisis should be kept only for the duration of the crisis. Afterward, most health data should be erased, though some non-identifiable information could be kept for historical, research, or public interest purposes.	😐The timeline for the protections is until the end of the public health emergency (Sec. 2(8)). As an initial matter, it might be necessary to extend that timeline because there may come a time when the virus still exists but we are no longer in a state of emergency. Regardless, data processed in response to COVID-19 should be kept only for the duration of the crisis, and non-identifiable data could be kept if it is only used for historical, research, or public interest purposes. The bill provides no protections for de-identified data that may be retained for any purpose and for any amount of time, and does not take into account potentially harmful uses of that data after the crisis is over.

Do not sell health data: Prohibit private companies from reusing or monetizing data.	😐The bill includes purpose limitations (Sec. 3(b)), yet it explicitly allows entities to transfer data to third parties without restriction (potentially for compensation).
Consider that **location data may be flawed**.	😟The bill permits, and thus encourages, the collection and use of precise geolocation and proximity data for purposes related to the virus even though geolocation data is likely not useful for COVID-related response. The bill also does not address the potential for mass surveillance through the collection of location data.
Require transparency and conduct mandatory **human rights impact assessments and due diligence processes** for every public-private partnership and public procurement.	😐The bill requires some transparency reporting but does not require human rights (or any kind of) due diligence or impact assessment (Sec. 3(c)(2)).
Allow for the **open and transparent review of products**.	😟The bill does not address the need for audits of software. Any private-sector application or technological solution to help fight COVID-19 should be open to full scrutiny of independent regulatory authorities and civil society groups.
All crisis response measures should be **transparent, necessary, and proportionate**.	😐While transparency is insufficient to protect people's privacy, it is still a necessary part of COVID-19 response. Privacy policies for COVID-19 apps should be 1) separate from the privacy policies the company may have for other services, 2) crystal clear on what data is collected, how it is used, and to whom it is transferred, and 3) provide specific information on data retention and security policies, rather than a "general description." The bill should also avoid preempting state laws or affecting other federal privacy laws, while also giving people the ability to file their own lawsuits.

For more information, please contact:

Eric Null, U.S. Policy Manager
eric@accessnow.org

Jennifer Brody, Legislative Manager
jennifer@accessnow.org

Isedua Oribhabor, U.S. Policy Analyst
isedua@accessnow.org

May 8, 2020