CENTER FOR
DEMOCRACY
& TECHNOLOGY

March 21, 2018

c/o Alaska House of Representatives
Judiciary Committee
Capitol Building
Juneau, AK, 99801

RE: HB 328 – Biometric and Geolocation Information Privacy

Dear Chairman Claman:

The Center for Democracy & Technology is a non-profit, non-partisan technology advocacy organization based in Washington, D.C., that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security online.

CDT appreciates the opportunity to express our support for HB 328. We believe this bill takes many positive steps toward protecting Alaskan's biometric and geolocation information.

CDT strongly believes that both biometric information and precise geolocation data are highly sensitive forms of personal data. While industry players have occasionally acknowledged the sensitivity of this information,[1] they often categorically state that any limitation on the collection of this data would inhibit innovation. Thus, companies continue to aggressively use geolocation data in ways that individuals may not expect,[2] and biometric information in ways that deny individual's ownership of their faces and voices. We believe that any collection and use of this information demands strong transparency from companies, as well as appropriate ways for individual Alaskans to control its collection and police corporate data practices. As HB 328 addresses biometrics and geolocation individually, we offer our comments about each data category separately.

Biometric Data

Biometric data is intrinsically sensitive and largely immutable; once it is breached, improperly shared, or used for tracking or surveillance, an individual is essentially stripped of their ability to protect their privacy. Companies and investors are devising new uses cases for biometric

[1] Automotive Privacy Principles, FAQ, Auto Alliance (2014), https://autoalliance.org/connected-cars/automotive-privacy-2/faq/.

[2] Christopher Mims, *Your Location Data Is Being Sold—Often Without Your Knowledge*, Wall St. Journal (Mar. 4, 2018), https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400 (noting that "as popular apps harvest your lucrative location data, the potential for leaking or exploiting this data has never been higher.").

information,[3] and 90% of employers intend to deploy biometric authentication by 2020.[4] However, there is a significant lack of transparency from vendors of biometric technologies about either their privacy practices or the security risks presented by their technologies.

This data is largely unregulated. The U.S. Government Accountability Office has acknowledged that there is "[n]o federal privacy law [that] expressly regulates commercial uses of facial recognition technology, and laws do not fully address key privacy issues stakeholders have raised, such as the circumstances under which the technology may be used to identify individuals or track their whereabouts and companions."[5] Only non-binding guidance is available governing certain uses of certain biometric data.[6]

Further, industry has become fiercely resistant to any attempt to establish common sense limits on these technologies.[7] Unfortunately, trade associations have come to see efforts to provide individuals with more information about the use of their own biometrics, and the ability to say "no," as a ban on the use of biometrics. Asking for permission does not shut down the development of biometric technologies -- it merely levels a very unequal playing field between companies and consumers.

State law can be an important mechanism for shaping deployment of biometrics. Legislative proposals in this area have generally attempted to describe technical processing functions that capture physical, physiological, or behavioral characteristics of an individual. As HB 328 acknowledges, biometric information can include fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual.[8]

We recommend additional specificity to the bill's provisions around "biometric data" and "biometric system." First, we suggest specifically adding facial recognition to this list of technologies. HB 328 may capture facial recognition through a catchall provision of "other physical characteristics," as well as its exception for photographs unless it "is collected for use

[3] April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, Wired (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

[4] Planet Biometrics, Nearly 90 Percent of businesses to use biometrics by 2020, (Mar. 20, 2018), http://www.planetbiometrics.com/article-details/i/6930/desc/nearly-90-percent-of-businesses-to-use-biometrics-by-2020/.

[5] Gov't Accountability Office, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law (GAO-15-621) (July 30, 2015), https://www.gao.gov/products/GAO-15-621.

[6] For example, the Federal Trade Commission issued a 2012 report looking at then-use cases for facial recognition with a significant emphasis on narrowly defined types of targeted marketing. Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[7] Justin Brookman, *CDT Withdraws from the NTIA Facial Recognition Process* (June 16, 2015), https://cdt.org/blog/cdt-withdraws-from-the-ntia-facial-recognition-process/; *see also* Jared Bennett, *Facebook: Your Face Belongs to Us*, Daily Beast (July 31, 2017), https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.

[8] H.B. 328, Sec. 18.13.290(1).

in a biometric system." However, an explicit reference to facial geometry may make HB 328 more clear, and explicitly covering facial recognition systems is important because they are likely to be one of the primary avenues in which individuals share their biometric data. Facial recognition and detection systems already are offered by major social networks[9] and, increasingly, in cameras and other consumer products.[10] When Apple began offering FaceID in the iPhone X last fall, it also began sharing certain types of facial mapping data with app developers.[11]

Second, the definition of "biometric system" may be more narrow than intended, limiting coverage to automated systems that "determines how well the extracted and stored biometric data match when compared under (D) of this paragraph and indicates whether an identification or verification of identity has been achieved."[12] This appears to exclude from HB 328 facial systems that detect race, gender, or other physical or emotional characteristics, even if they tie this information to a unique biometric identifier. While such systems do not "identify" a user against a database of images or otherwise verify identity, they can be used to track individuals across different times and locations without their knowledge. This sort of data can have tremendous utility to advertisers and retailers. For instance, a University of Toronto study has shown that facial cues can be used to identify an individual's socioeconomic status.[13] Algorithms that sift-through facial data can also correctly identify sexual orientation among men in 81% of cases and 74% of cases among women given a single facial image.[14]

Geolocation Data

Like biometric data, geolocation information is highly sensitive.[15] A user's location divulges intimate personal details, including where individuals worship, when they seek out health treatments, and how they go about their daily lives, facilitating inferences about their lifestyle, habits, and relationships.[16] This information is incredibly valuable; marketers spent $16 billion on location-targeted ads served to mobile devices like smartphones and tablet computers in

[9] Rob Sherman, *Hard Questions: Should I Be Afraid of Face Recognition Technology?*, Facebook (Dec. 19, 2017), https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/.
[10] Dieter Bohn, *The Google Clips Camera Puts AI Behind the Lens*, The Verge (Oct. 4, 2017), https://www.theverge.com/2017/10/4/16405200/google-clips-camera-ai-photos-video-hands-on-wi-fi-direct.
[11] Kate Conger, *What's Really Up With Apple Giving Face Data to Developers?* (Nov. 2, 2017), https://gizmodo.com/whats-really-up-with-apple-giving-face-data-to-app-deve-1820085175.
[12] H.B. 328, Sec. 18.13.290(3)(E).
[13] RT Bjornsdottir et al., *The Visibility of Social Class From Facial Cues* (2017), *available at* https://www.ncbi.nlm.nih.gov/labs/articles/28557470/.
[14] Yilun Wang & Michal Kosinski, *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images* (2017), *available at* https://osf.io/zn79k/.
[15] 82% of those surveyed stated they considered their physical location over time to be sensitive information. Mary Madden, Pew Research Center, Americans Consider Certain Kinds of Data to be More Sensitive than Others (2014), http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/.
[16] Press Release, FTC Testifies on Geolocation Privacy, FTC (June 4, 2014), https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy.

2017.[17] Applications ranging from weather apps,[18] flashlights,[19] and dating services[20] all traffic in location data.

Location information is also highly identifiable and not easily anonymized. An analysis of 15 months of anonymized mobile phone data discovered that only four spatio-temporal data points are needed to uniquely identify 95 percent of users.[21] More recently, researchers from the University of Washington were able to utilize mobile advertising networks in order to track a target's location in real-time and even determine what apps they used and when.[22] These sorts of tracking technologies have become incredibly sophisticated and opaque. While individuals have come to understand the connection between device location-services powered by GPS, it is less obvious other methods in which geolocation can be derived.[23]

As with biometrics, precise definitions of "geolocation" are rare. While HB 328 explicitly excludes IP addresses, common sources of geolocation data range from GPS information to information derived from other network signals such as RFID, WiFi and Bluetooth MAC addresses, and GSM/CDMA cell IDs, as well as user inputs.[24] As a result, legislative efforts tend to address geolocation by covering a range of sources when used to determine location with certain precision.

We believe that HB 328's definition of "geolocation information" can be clarified. Excluding IP addresses, the definition includes *any* "information identifying the geographical location of a person or device by using digital information." As a result, this proposed definition does not appear to distinguish between precise and imprecise location information. An overbroad definition of any type of geographical information attached to a person or device could inadvertently capture apps or services such as a clock providing time zone information.

We would point to a recent proposal in California, Assembly Bill 83, which offers a more limited definition of covered geolocation data: "Location data generated by a consumer device capable

[17] Mims, *supra* note 2.
[18] Taylor Hatmaker, *AccuWeather updates its iOS app to address privacy outcry*, TechCrunch (Aug 24, 2017), https://techcrunch.com/2017/08/24/accuweather-update-reveal-mobile/.
[19] Press Release, Fed. Trade Comm'n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.
[20] Matt Burgess, *Top iOS dating apps are exposing your personal life to hackers*, Wired (Feb. 9, 2017), www.wired.co.uk/article/the-dating-apps-exposing-your-personal-life-to-hackers.
[21] Yves-Alexandre de Montjoye, *Unique in the Crowd: The privacy bounds of human mobility* (Mar. 25, 2013), https://www.nature.com/articles/srep01376.
[22] ADINT: Using Targeted Advertising for Personal Surveillance (2017), https://adint.cs.washington.edu.
[23] Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.
[24] Ctr. for Democracy & Tech., Guide to Defining Technical Terms in State Privacy Legislation (June 2017), https://cdt.org/insight/cdts-guide-to-defining-technical-terms-in-state-privacy-legislation/.

of connecting to the Internet that directly identifies the precise physical location of the identified individual at particular times and that is compiled and retained."[25] This definition protects information that can most directly identify an individual and provides a limited, workable definition for companies.

--

CDT lauds Alaska for taking steps to return control over personal information to its citizens. HB 328 empowers users to make informed choices about the collection, use, and disclosure of highly sensitive personal information. Companies who chose to deploy systems that rely on biometric and precise geolocation information must be held to a high standard of data protection. We believe this bill's provisions will improve industry practices and restore consumer trust in these technologies.

Thank you again for the opportunity to comment on HB 328. Please contact me at jjerome@cdt.org or 202.407.8812 with any questions.

Sincerely,
Joseph Jerome
Policy Counsel, Privacy & Data Project
Center for Democracy & Technology

[25] CA AB 83, Personal Data (2015), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB83.