HB

328

<TARGET><BILL>HB 328</BILL><SUBJECT>HB 328</SUBJECT><COMM>HJUD30</COMM></TARGET>

Alaska State Legislature

Representative Matt Claman

Session: State Capitol, Rm 118 Juneau, AK 99801 Phone: 465-4919
Interim: 1500 W. Benson Blvd., Anch, AK 99503 Phone: 269-0130

House Bill 328
Sponsor Statement

"An Act relating to biometric information and to the collection, use, storage, and disclosure of geolocation information; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

Increasingly, geolocation data, information about a person's whereabouts generated as a biproduct of their use of a mobile device, and biometric data, information based on biometric identifiers like finger prints and facial scans, are being collected and used for commercial applications ranging from security to tailored advertising. While some of these applications may be welcome, especially to the companies that collect and use the data, others can be harmful to the individual whose data is collected.

Biometric identifiers, unlike a password or an email address, cannot be changed. If compromised, they are compromised for good. Biometric information, when used in a commercial setting, has the potential to allow for discriminatory practices based on appearance. Knowing where a person is located often means knowing what that individual is doing. Geolocation data may not always be information a person wants available to private companies, ranging from advertisers to potential employers. Unregulated geolocation data and biometric information not only threaten an individual's privacy, but also threaten freedom of expression and association. House Bill 328 seeks to ensure that geolocation and biometric information are collected, disseminated, and stored in a responsible, transparent way.

House Bill 328 will require private entities collecting biometric data to inform subjects that the information is being collected, and the specific purpose and length of time for which the data will be used. Private entities will be required to obtain a written release from the individual before collecting this information. They may not profit from a person's biometric information or share this information, except at the subject's request or in an instance where a warrant has been issued. In the case of geolocation data collection, companies will be required to inform individuals that the data will be collected, the specific purpose for which the data will be used, and where they can view this information. Through these measures, House Bill 328 will give Alaskans greater control over the way their personal digital information is being collected and used.

Staff Contact: Ceri Godinez
Ceri.Godinez@akleg.gov

Alaska State Legislature

Representative Matt Claman

Session: State Capitol, Rm 118 Juneau, AK 99801 Phone: 465-4919
Interim: 1500 W. Benson Blvd., Anch, AK 99503 Phone: 269-0130

House Bill 328
Sectional Analysis—Version A

Section 1
Adds new sections to AS 18.13:
Requires that, before collecting an individual's biometric data, the collector notify the individual that the data is being collected, the purpose for which it is being collected, and the length of time for which it will be stored; and receives the individual's consent to these terms, which the individual can revoke or amend at any time. The collector may only disclose biometric information to the collector's contractor or for the purpose of authenticating the identity of the individual providing the information and may only disclose the information for the original purpose the individual consented to or for a fraud prevention purpose. Collectors may not sell biometric information. When the biometric information is no longer needed, it must be removed from all databases and destroyed within 120 days. Persons found to have intentionally violated any of these requirements are liable for $1,000 except in cases where the violation resulted in profit in which case the penalty is $5,000. Exemptions to these collection, retention, and disclosure requirements include biometric information used for law enforcement purposes, biometric information authorized by state or federal law, facial images for state IDs, photographs, and voices recorded for quality assurance purposes.

Section 2
Adds new sections to AS 45.48:
Requires that, prior to collecting, using, storing, or disclosing an individual's geolocation information, a person notify the individual that the information will be collected and the purpose for which it will be collected, provide an easy online means for accessing the information collected, and obtain express consent to the disclosure. Exceptions to this include situations where a private person collects its own geolocation information, a parent is attempting to locate a child, a court-appointed guardian is attempting to locate an incapacitated person, and a person is attempting to provide emergency services; and entities including utilities that furnish telecommunications services, health care providers subject to P.L. 104-191, and financial institutions subject to 15 U.S.C 6801-6809. Persons found to have intentionally violated any of these requirements are liable for $1,000 or the total value of the damages incurred, whichever amount is greater, and any other relief the court deems appropriate.

Section 3
Amends AS 45.50.471 (b) to include violation of geolocation information protection under the terms "unfair methods of competition" and "unfair or deceptive acts or practices."

Section 4
Applies sections added to AS 45.48 under Section 2 of this bill to contracts entered into on or after the effective date of this Act.

Section 5
Replaces "this chapter" with "AS 18.13.010 – 18.13.100" whenever it appears in AS 18.13.010 – 18.13.100 which relates to genetic testing privacy.

Fiscal Note

State of Alaska
2018 Legislative Session

Bill Version: HB 328
Fiscal Note Number:
() Publish Date:

Identifier: HB328-LAW-CIV-03-16-18
Title: BIOMETRIC/GEOLOCATION INFO/TRADE PRACTICE
Sponsor: CLAMAN
Requester: House Judiciary

Department: Department of Law
Appropriation: Civil Division
Allocation: Commercial and Fair Business
OMB Component Number: 2717

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2019 Appropriation Requested	Included in Governor's FY2019 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2019**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimated SUPPLEMENTAL (FY2018) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2019) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version/comments:

Not applicable, initial version.

Prepared By: Valerie Rose, Budget Analyst — Phone: (907)465-3674
Division: Administrative Services Division — Date: 03/16/2018 10:53 AM
Approved By: Jahna Lindemuth, Attorney General — Date: 03/16/18
Agency: Department of Law

FISCAL NOTE ANALYSIS

STATE OF ALASKA **BILL NO.** HB 328
2018 LEGISLATIVE SESSION

Analysis

HB 328 would establish a new article in AS 18.13, genetic privacy, that puts restrictions on the use of biometric data. A person who collects biometric data must notify the individual in a clear manner of the collection and specific purpose for which the biometric information will be used. The bill would add provisions related to the disclosure, sale, use, and storage of biometric information. In addition, the bill allows a person to bring a civil action against a person who intentionally violates the provisions on the collection and use of biometric information. The bill exempts collection of biometric information for (1) law enforcement purposes, (2) if allowed under state and federal law, (3) for issuance of state identification cards and other identification purposes, such as driver's licenses, photographs (unless collected for use in a biometric system) or voice recordings retained for quality assurance.

The bill adds provisions on the collection, use, storage, and disclosure of geolocation information to AS 45.48 which governs competitive practices and consumer protection. New AS 45.48.800 would prohibit a private person from collecting, using, storing, or disclosing biometric information on a person's individual mobile electronic device unless the private person provides the individual written notice and the individual consents to the disclosure. Both the requirements for notice, and exemptions from the need for notice, would be set out in statute. A violation of the requirements for collection, use, storage, and disclosure of geolocation information would be actionable as an unfair or deceptive act under AS 45.48.850; under that new statute the individual could recover liquidated damages of $1,000 or actual damages, whichever is greater, and other relief the court deems appropriate. An individual could not bring a class action for violation of AS 45.48.800 – 45.48.880.

Sec. 3 of the bill makes a violation of geolocation information an unfair or deceptive practice under AS 45.50.471, which would allow the Department of Law to investigate and bring an action for injunctive relief and civil penalties. This would also allow private consumers to bring a civil action to recover treble damages or $500, whichever is greater, and other relief a court considers necessary and proper.

The department expects a limited increase in work but would expect it could be absorbed into existing resources.

Lizzie Kubitz

From: Noah Williams <noahsbwilliams@gmail.com>
Sent: Tuesday, February 06, 2018 8:09 AM
To: Rep. Matt Claman
Subject: Biometric Privacy Bill specifics

Representative Claman,

In principle I support your bill to safegard the personal data of Alaskans-but I feel it needs a provision of corcing cellular carriers to offer users a complete opt-out of all geolocation data services. The physical way in which cell phones are designed allows carriers practically unlimited access to devices (learn more about this here), so giving consumers both full transparancy and the capacity to opt-out of location data collection is essential. This is especially true in many areas of Alaska where one cellular carrier (GCI or AT&T) owns a complete monopoly over the cellular infrastructure and/or services.

Thank you for standing up for our rights

Be well,
—Noah Williams
(907)465-7291
District 33

BIOMETRICS ARE COMING, ALONG WITH SERIOUS SECURITY CONCERNS

YOU'RE BUYING A pair of jeans. At the register, instead of reaching for your wallet or phone, you pull back your hair. The cashier holds a camera up to your ear. The camera confirms a match to a photo in a database, all of which is linked to your bank. Transaction complete.

This futuristic scenario is actually not so far-fetched, and it's coming sooner than you might think. Research on biometric tech has amped up, leading to mobile apps that read various unique-to-you body parts to help verify your identity, raising all kinds of security and privacy concerns, and it's still an open question as to how government and manufacturers are going to address it all.

But back to that ear scan. "Ears are unique," says Michael Boczek, the President and CEO of Descartes Biometrics, a company that specializes in mobile ear detection security apps. "It's stable and enduring, which means it changes very little over the course of one's life. That's also true of fingerprints, but less true of facial recognition."

Just because someone might be able to use their ear at checkout doesn't mean it's necessarily going to happen anytime soon, though. "Biometrics are tricky," Woodrow Hartzog, an Associate Professor of Law at Samford University told WIRED. "They can be great because they are really secure. It's hard to fake someone's ear, eye, gait, or other things that make an individual uniquely identifiable. But if a biometric is compromised, you're done. You can't get another ear."

Databases get hacked all the time, from the IRS to Target to hospitals and banks, and until some of the very real security concerns surrounding the use of biometric technologies are better ironed out, you wouldn't be wrong to worry about linking data about your body parts to online accounts.

Biometrics? Back Up

Biometric identification refers to any technology that does one of two things: identifies you or authenticates your identity. For identification, an image is run against a database of images. For authentication, an image has to be accessed from the device to confirm a match. The latter is typically used for unlocking computers, phones, and applications.

Since Apple introduced its incredibly usable biometric identification with Apple's home button fingerprint sensor in 2013, the appetite for biometrics has expanded rapidly. Now MasterCard wants to use your heartbeat data to verify purchases. Google's new Abicus Projectplans to monitor your speech patterns, as well as how you walk and type, to confirm that it's really you on the other end of the smartphone. Other apps are looking at the uniqueness of vascular patterns in the eyes or even a person's specific gait to verify identities.

The idea isn't actually new. Police have been fingerprinting for over 100 years and have used digital biometric databases since the 1980s. But until the 2013 iPhone, consumer-level biometric verification was largely limited to unlocking devices with fingerprints. And those sensors were in awkward places, like on the back of a phone or next to the trackpad on laptops.

Mobile biometrics have also piqued the interest of investors. Reports surfaced that the Swedish biometrics company responsible for fingerprint identification in most Android devices, Fingerprint Card AB, saw a 1,600 percent increase in its stock in just the last year alone, making the company one of the best performing stocks in Europe in 2015.

Securing the Public

Although many experts say biometrics are intrinsically secure (since no one else can have your ears or eyes), Alvaro Bedoya, Professor of Law at Georgetown University, argues otherwise. "A password is inherently private. The whole point of a password is that you don't tell anyone about it. A credit card is inherently private in the sense that you only have one credit card."

Biometrics, on the other hand, are inherently public, he argues. "I do know what your ear looks like, if I meet you, and I can take a high resolution photo of it from afar," says Bedoya. "I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass." And that makes them easy to hack. Or track.

Law enforcement agencies are particularly aware of how public your body parts actually are. A technology like that ear-scan, which can be used to make shopping easier in one scenario, can be used by the police in another. The FBI has been building a biometric recognition database that it hoped to have filled with 52 million facial images by 2015, with thousands more images added every month. The Department of Homeland Security is working with U.S. Customs and

Border Patrol to add iris scans and 170 million foreigner fingerprints to the FBI's national database. And local police departments are also in on the biometrics game. The *LA Times *reported that the police department in Los Angeles invested millions of dollars in 2015 to expand biometric identification capabilities for officers in the field, and according to research from the Electronic Frontier Foundation, numerous other police departments have mobile fingerprint identification already deployed.

Even Boczek says that police are interested in his ear verification software. He explained that it would allow a police officer with a body-mounted camera that sits mid-chest to capture images of someone's ear to scan when they approach a driver's window. In fact, he says this technology is currently being tested by police departments in Washington state.

Writing the Rules

The use of data about your body parts is largely unregulated.

Last summer, the National Telecommunications and Information Administration held a workshopto craft a voluntary code of conduct for the operation of facial recognition technology. Trade associations were there, representing companies like Google and Microsoft, as well as advocates and experts. But they didn't get far. Before the meeting was over, everyone from the public interest community walked out.

"Not a single trade association would agree that before you use facial recognition to identify someone by name, even if you don't have any relationship with that person, you need to get their consent," said Bedoya. "The industry associations in the room were taking a position that was well beyond standard practices."

The US government is dancing around the question of consent and how to oversee biometrics, with what seems like almost every agency in Washington addressing part of the issue. The National Institute of Standards and Technology has been evaluating the efficacy of biometric identification for years, focusing on face identification, fingerprint, voice, and iris scans. The Federal Trade Commission is leading the charge on data security. The FDA deals with the security of implantable devices, and the Department of Health and Human Services handles personal health information.

For now, it's legal in 48 states for software to identify you using images taken without your consent while you were in public. Texas and Illinois don't allow it for commercial use, but it's legal nationwide for law enforcement. And even

when consent is obtained, it's often done so in a way you may not be aware of: in the fine print of Terms of Service agreements that people routinely don't read.

"The law is written in such a way that that these agreements are routinely considered valid and that they are the way for companies to get permission to collect, use, and share your personal information," says Hartzog.

But companies have been self-regulating for sometime now. Google Executive Chairman Eric Schmidt, as Bedoya notes in an article he wrote for Slate, even once said that facial recognition was "the only technology Google has built and, after looking at it, we decided to stop." Microsoft's Xbox and Apple's iPhoto both have limited uses of the software on an opt-in only basis. We reached out to Apple and Google about this, but neither had comment. Microsoft responded that it keeps facial recognition opt-in because the company believes "it's important to be able to personalize and control your Xbox experience."

And then there's Facebook. With over 350 million photos uploaded every day, the company's research lab suggests that it has "the largest facial dataset to date"—powered by DeepFace, Facebook's deep learning facial recognition system, but Facebook has an agreement with the FTC that says it first has to first obtain "affirmative express consent" before going beyond a user's specified privacy settings.

Bedoya says, using such a system, it's not hard to imagine a future where someone walks into a car dealership, and immediately the dealership knows who they are, where they live, their income, their credit score—all thanks to Facebook. After all, there's already facial recognition software that brick-and-mortar shops can use to identify "return shoppers" and signal when "pre-identified shoplifters" enter the store.

Creepy, Public, and Unsafe?

Just as you can buy software to brute force your way through pins and passwords, hackers are already engineering ways to spoof biometric authentication. One of the big reasons we're not all using our bodies to verify purchases now is that the security isn't there yet.

When the Office of Personnel Management was hacked last year, 5.6 million people's fingerprints were compromised. Universities are hacked every year, medical records, the IRS, banks, dating websites, the list goes on. Biometric data isn't immune to these attacks. In fact researchers from mobile security firm Vkansee were able to break into Apple's Touch ID system with a small piece of

Play Doh just last month at the Mobile World Congress—similar to what security researcher Tsutomu Matsumoto a did with a gummy bear over a decade earlier with another fingerprint sensor. And researchers at Michigan State University just last month released a paperthat describes a method for spoofing a fingerprint reader using conductive ink printed with an ink jet printer in less than fifteen minutes.

Beyond the security question, there's also something just plain creepy about the technology. Case in point: MasterCard has partneredwith the biometrics company Nymi to test heartbeat authentication for credit card purchases. (That would be in addition to its selfie-and-fingerprint payment verification app it rolled out at Mobile World Congress). Or EyeVerify, which works by scanning the blood vessel patterns in the whites of your eye by using a selfie taken with a smartphone. Other mobile phone companies have built devices that use infrared cameras to scan irises.

"There's a question as to how viscerally people will respond to biometrics. The fingerprint reader seems to have caught on pretty well, because it was really useful and easy," says Hartzog. "When people feel creeped out they may be less gung-ho to adopt some kind of biometric."

And if you can get past the ick factor, then there's also the privacy question. Are you willing to use your unique bodily identifiers to link you to a purchase history? Think about how often you purchase items you'd rather keep private: porn, alcohol, drugs, condoms, a hoverboard.

"We enjoy shopping in relative obscurity," says Hartzog. "This is something that we might be able to accept for some purchases, but for it to be standard practice in America strikes me as a long way off." If you knew the political thinking of everyone you bought things from, you'd probably be slightly disturbed. As University of Washington law professor Ryan Calo expressed in a recent paper, a certain level of privacy allows us to do business with each other; it's part of interacting in a marketplace.

"We're probably not ready to hand over the keys to the entire biometric kingdom when we're not sure how this is going to work," Hartzog added. Eventually, we may be willing to exchange privacy for the convenience—but not just yet.

DOW JONES, A NEWS CORP COMPANY

DJIA **24610.91** -1.35% ▼ Nasdaq **7344.24** -1.84% ▼ U.S. 10 Yr **-3/32 Yield** 2.857% ▼ Crude Oil **62.09** 0.05% ▲ Euro **1.2336** 0.01% ▲

THE WALL STREET JOURNAL.

https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400

KEYWORDS

Your Location Data Is Being Sold—Often Without Your Knowledge

Location-based ads are growing, which means the industry has more ways than ever to track you

Businesses and other locations, in green, where the location-based advertising firm Groundtruth pushes ads to mobile devices.
PHOTO: KENNETH BACHOR/THE WALL STREET JOURNAL

By

Christopher Mims
March 4, 2018

As location-aware advertising goes mainstream—like that Jack in the Box ad that appears whenever you get near one, in whichever app you have open at the time—and as popular apps harvest your lucrative location data, the potential for leaking or exploiting this data has never been higher.

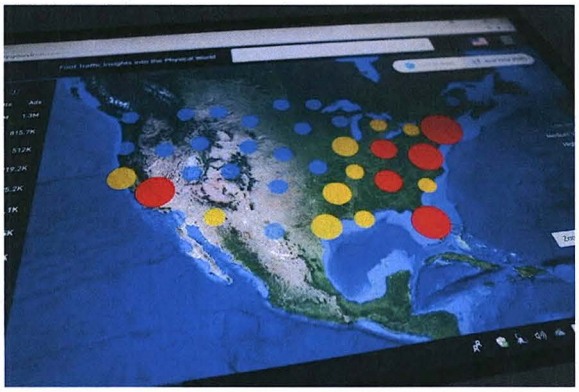
It's true that your smartphone's location-tracking capabilities can be helpful, whether it's alerting you to traffic or inclement weather. That utility is why so many of us are giving away a great deal more location data than we probably realize. Every time you say "yes" to an app that asks to know your location, you are also potentially authorizing that app to sell your data.

Dozens of companies track location and/or serve ads based on this data. They aim to compile a complete record of where everyone in America spends their time, in order to chop those histories into market segments to sell to corporate advertisers.

Marketers spent $16 billion on location-targeted ads served to mobile devices like smartphones and tablet computers in 2017. That's 40% of all mobile ad spending, research firm BIA/Kelsey

estimates, and it expects spending on these ads to double by 2021.

The data required to serve you any single ad might pass through many companies' systems in milliseconds—from data broker to ad marketplace to an agency's custom system. In part, this is just how online advertising works, where massive marketplaces hold continuing high-speed auctions for ad space.



A map of the U.S., showing areas of unusually high visits to sites where location-based advertising firm Groundtruth pushes ads to mobile devices. PHOTO: KENNETH BACHOR/THE WALL STREET JOURNAL

But the fragmentation also is because of a very real fear of the public backlash and legal liability that might occur if there were a breach. Imagine the Equifax breach, except instead of your Social Security number, it's everywhere you've been, including your home, your workplace and your children's schools.

The fix, at least for now, is that with most individual data vendors holding only parts of your data, your complete, identifiable profile is never all in one place. Giants like Facebook and Alphabet 's Google, which do have all your data in one place, say they are diligent about throwing away or not gathering what they don't need, and eliminating personally identifying information from the remainder.

Yet as the industry and the ways to track us expand, the possibility that our whereabouts will be exposed multiplies. If you've ever felt clever because an app on your phone asked to track your location and you said no, this should make you feel a little less smug: There are plenty of ways to track you without getting your permission. Some of the most intrusive are the easiest to implement.

The spy in your pocket

Your telco knows where you are at all times, because it knows which cell towers your phone is near. In the U.S., how much data service providers sell is up to them.

Another way you can be tracked without your knowing it is through any open Wi-Fi hot spot you might pass. If your phone's Wi-Fi is on, you're constantly broadcasting a unique address and a history of past Wi-Fi connections. Retailers sometimes use these addresses to identify repeat customers, and they can also use them to track you as you go from one of their stores to another.

WeatherBug, one of the most popular weather apps for Android and iPhone, is owned by the location advertising company GroundTruth . It's a natural fit: Weather apps need to know where you are and provide value in exchange for that information. But it also means that app is gathering data on your location any time the app is open—and even when it isn't, if you agreed to always let it track your location. That data is resold to others.

Jack in the Box pushes promotions to apps on potential customers' mobile devices when they are near its stores. PHOTO: LUKE SHARRETT/BLOOMBERG

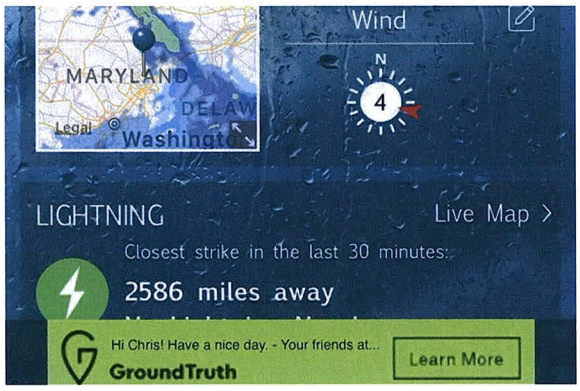
GroundTruth also says it gathers location data from "over a hundred thousand" other apps that have integrated bits of its code. Company President Serge Matta declined to disclose which apps. App makers agree to harvest location data because it grants them access to GroundTruth's mobile advertising network.

This data is what enables marketers like Jack in the Box to push an advertiser's message to potential customers near its restaurants. A typical engagement includes pushing location-based promotions or coupons through mobile ads, says Iwona Alter, chief marketing officer of Jack in the Box.

Every month GroundTruth tracks 70 million people in the U.S. as they go to work in the morning, come home at night, surge in and out of public events, take vacations, you name it.

Anonymize, de-anonymize

Companies like GroundTruth try to ensure they aren't tracking or storing data on individuals. Most of what they sell are anonymous blobs of people who fit particular descriptions—"soccer moms who intend to buy an SUV," for example. But they also occasionally hand off location data to a third party, such as LiveRamp, owned by data broker Acxiom , before it is matched up with potentially personally identifying information, such as your complete shopping history at a retailer. LiveRamp is almost like an escrow company for data.



GroundTruth demonstrated its ability to target a mobile ad to a single location by pushing this message to everyone at the Starbucks where columnist Christopher Mims was working. Ordinarily, these ads would not contain personalized messages or personal information. PHOTO: CHRISTOPHER MIMS/THE WALL STREET JOURNAL

Companies like Acxiom could be prime targets for hackers, said Chandler Givens, chief executive of TrackOff, which develops software to protect user identity and personal information. LiveRamp goes to great lengths to mathematically obfuscate our individual identities, said Sheila Colclasure, chief data ethics officer at LiveRamp and Acxiom. But some security researchers fear data brokers like Acxiom might be compromised already, or could be someday.

Acxiom and LiveRamp in the U.S. are governed by federal and state laws that regulate the collection and use of data in the particular businesses their clients are involved in, Ms. Colclasure said. Nearly every year, a bill comes up in the Senate or House that would regulate our data privacy—the most recent was after the Equifax breach—but none has passed. In some respects, the U.S. appears to be moving backward on privacy protections.

There might never be a breach of our location data. But given the drumbeat of hacks of both companies and governments, it's hard to believe hackers aren't at least trying to compromise such a high-value target.

Write to Christopher Mims at christopher.mims@wsj.com

Corrections & Amplifications

GroundTruth's marketing materials and representatives say the company gets data from "over a hundred thousand" other apps. An earlier version of this article incorrectly attributed this figure to GroundTruth President Serge Matta. (March 4, 2018) Also, a caption with an earlier version of this column didn't make clear that GroundTruth's ads don't ordinarily contain personalized messages or personal information. (March 5)

Appeared in the March 5, 2018, print edition as 'You're Being Tracked, and Hackers Loom.'

Forbes / Tech

BETA

DEC 24, 2014 @ 03:04 PM 4,997

BEWARE: The Dangers Of Location Data

Danielle Citron, CONTRIBUTOR

FULL BIO

Opinions expressed by Forbes Contributors are their own.

This week, California Attorney General Kamala Harris HRS -1.06% advised her constituents to disable their phones' automatic location identifier. Consumers likely don't know that their phones continuously collect their location data for reasons that have nothing to do with the routing of their calls and e911 requirements. Her advice is to turn off the default, the always on setting, and turn it on for specific uses. You want to let Yelp YELP -0.71% ! know where you are--sure, give the app permission for a specific moment in time. Otherwise, turn it off.

That is wise advice. If consumers keep the always-on setting for their geolocation data (that is, the street and city where a phone is located as it changes moment to moment), they are opening themselves up to mischief and far worse. Geolocation data tells us intimate, revealing details about people's lives--their visits to drug treatment clinics, psychiatrists, prospective employers, and more. As AG Harris told USA Today, "Broadcasting your location can sometimes expose you and your family to risk of theft or physical harm. . . For instance, you may be unknowingly revealing your location if your phone is 'geo-tagging' your photos. ... Sharing a 'selfie' without disabling geo-tagging can be dangerous, especially for victims of stalking or domestic abuse." Companies can sell geolocation data to data brokers, further filling their dossiers with information about consumers' medical conditions, religious affiliations, and more.

Consumers may well be giving mobile apps access to their geolocation data without ever having given specific permission. Indeed, most mobile apps are not transparent about the fact that they collect geolocation data. Most mobile app companies say that they only collect geolocation data after getting express consent from consumers, but that is not the case. As the FTC's Director of the Bureau of Consumer Protection Jessica Rich testified this past summer before a Senate Privacy, Technology, and Law subcommittee hearing, companies often claim that they have an opt-in approach to geolocation data but do not follow it in practice. The Flashlight app and

Snapchat cases show that opt-in standard is not the norm. For instance, Snapchat transmitted geolocation information from users of its Android app, even though its privacy policy claimed it did not track users or access such information. The developer of a flashlight app failed to disclose that its app transmitted the device's location to third parties, including mobile ad networks. The company and its manager agreed to an order that prohibits them from misrepresenting how consumers' information is collected and shared. Crucially, the company must obtain consumers' affirmative express consent before collecting, using, and sharing their geolocation data.

As privacy scholars Daniel Solove and Woodrow Hartzog powerfully argue, the FTC's consent decrees establish common law set of principles. Recent FTC settlements in cases involving CyberSpy Software, Flashlight app, and Snapchat app make clear that geolocation data is the third rail. Be careful before collecting it and take certain steps if you do. Geolocation data is especially revealing about our lives. It is subject to serious abuse, from domestic abuse and stalking to theft and discrimination. Mobile apps and other entities should get express consent from consumers before collecting it. They should not share it with any entity without consumer consent. I'll have more to say about the criminal consequences of stalking apps later but for now there is much consumers and mobile app providers need to do to respect privacy.

The Risks of Voice Technology

by Katherine Heires | October 2, 2017 at 6:08 am

These days, voice technology is everywhere. Voice-enabled digital devices and virtual assistants from Amazon, Apple, Google, Microsoft and others can answer a question, provide a weather report, turn up the thermostat or even order a pizza. Businesses are using voice technology to improve call center performance, verify customer account information and assist workers on the job.

Described as "the next paradigm shift in IT" by Gartner Research, voice technology use is booming both at home and in the workplace. "Spoken interfaces are proliferating and successful implementations can reduce operating costs while improving customer experience," said Dan Miller, lead analyst and founder of Opus Research, an analysis firm focused on intelligent assistance including voice technology.

As of the end of 2016, he estimated, more than 1,200 companies had implemented nearly 2,700 intelligent technology products, 400 of which are voice-enabled, with many more to come. Indeed, according to an IHS Markit report, the AI-powered digital assistance market—which includes voice-enabled devices—is on track to exceed four billion consumer devices by the end of 2017 and will grow to more than seven billion by 2020.

"Voice is finally breaking through as the next interface," said Peter Cahill, founder and CEO of Voysis, a Dublin-based software firm.

Voice-enabled technology has been around for ages—IBM, for example, has been working on it for decades. But it was the more recent success of virtual assistants like Apple's Siri and Amazon's Alexa that really helped put voice technology in the spotlight. Now, the use of voice-enabled technology is becoming increasingly common. Indeed, Gartner Research predicts that 20% of smartphone interactions will occur through intelligent assistants in 2019, and by 2020, a majority of all tech devices will be designed to work with voice control.

"Consumers are becoming increasingly comfortable with the technology, which is driving engagement," said Martin Utreras, vice president of forecasting at eMarketer. "As prices decrease and functionality increases, consumers are finding more reasons to adopt these devices." Walmart, for example, recently partnered with Google to enable voice-controlled purchasing.

Talking About Risks

While more people are readily introducing these devices into both home and business settings, experts warn of the risks and challenges associated with voice technology. "The addition of voice absolutely increases the risk level for technology users," said Nathan Wenzler, chief security strategist at AsTech

Consulting, a cyberrisk management firm. "When you add more features to a device, you are also adding complexity and more code and, as a result, you are introducing more avenues for people to hack into the device. It's a major risk component."

"The minute you have microphones in people's offices, you are creating a situation where other people will want to listen in."

Most devices that employ voice-response technology are internet of things devices and, like many data-collecting devices in this nascent category, manufacturers often do not embed adequate security measures into them. "It can be very easy to break into voice-enabled IoT devices and compromise them, and that opens up a lot of problems," he said.

One such concern is the vulnerability of any device that uses voice as a biometric identification factor. "I can trick the device into thinking I am you or I can intercept your voice and then use your voice print for other purposes," Wenzler said. Your voice is essentially a password, but since you cannot change or alter it easily, once compromised, its effectiveness for security disappears.

Just as the quality of voice recognition and verification technology has improved, so has the ability to spoof or mimic someone else's voice for nefarious purposes, according to Dr. Alexander Rudnicky, professor in the Language Technologies Institute at Carnegie Mellon University's School of Computer Science. This can result in serious misuse and fraud in the form of "replay attacks," where a voice is replicated and then replayed to allow access to financial accounts, work facilities or virtual assistants.

Voice-enabled technology also raises serious privacy concerns. "Many voice-enabled technologies have always-on microphones and are listening to pretty much everything you say," said Matthew D. Green, an assistant professor of computer science at John Hopkins University's Information Security Institute. Although these devices are usually waiting to hear a "wake word" that activates them to listen and respond to a voice command, there is still a possibility that voice data can be exposed. "This definitely creates a privacy risk in corporate environments where your phone may be activated in error and what you thought was a private conversation is sent to Google in the cloud," he said.

Should hackers then break into the devices or the cloud systems where the data is stored, they could access these private conversations. "The minute you have microphones in people's offices, you are creating a situation where other people will want to listen in," Green said. Businesses with voice data that must be protected from competitors' prying ears should especially be thinking about these types of risks.

Many companies are sensitive to these concerns and offer customers the option to disable voice data collection or delete such data. "Customers can turn any data capture off, in which case we toss the data," said Michael Picheny, senior manager at the IBM TJ Watson Research Center, of IBM's policy. In the case of the Amazon Echo device, customers have the option to go through the Amazon website to delete

the questions they have asked Alexa, though the company advises that doing so may inhibit the quality of service.

Earlier this year, these privacy issues came to light when prosecutors in Arkansas sought voice recordings collected by an Echo device as part of a murder investigation. Amazon initially turned down the request for the data, saying in a statement, "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course." Amazon eventually released the data when the defendant expressed a willingness to do so, but the case is likely only the first of many such conflicts to come between individuals, providers of voice-enabled technology and the courts over privacy rights.

Addressing the Concerns

Businesses thinking about using or developing voice-enabled capabilities must also be aware of the challenges of data collection. "Voice print collections are no different from other types of personal information that need to be protected," said Larry Ponemon, chairman and founder of the Ponemon Institute.

> "Voice print collections are no different from other types of personal information that needs to be protected."

Ideally, encryption methods should be used so that the data cannot be easily accessed by cyber criminals, he said. Global businesses also need to be aware of the increased risk coming with the requirements of the European Union's General Data Privacy Regulations (GDPR), which go into effect in May 2018 and impose strict rules on business regarding the protection of EU citizens' personal data, including protection against unauthorized or unlawful processing, data breaches or accidental loss of data.

The new law will impose fines of up to €20 million (about $24 million) or 4% of a firm's global annual turnover for the preceding year, whichever is greater, for any infractions. The risk for many businesses, Ponemon said, is that their chief privacy officer may be focused on protecting more traditional types of information without thinking about newer types of data that also fall under the regulation, such as voice data.

There are several strategies to counter the risks associated with voice technology. For example, to protect against voice spoofing, speech and biometrics consultant Dr. Judith A. Markowitz recommends that companies implement security systems that use multifactor authentication, rather than relying solely on voice. "If you are using speaker verification but are still unsure about the person's identity, you can use another biometric as a backup," she said. Companies should also assess the importance of the data being protected to determine how secure it needs to be. "If it is something that requires high security, then you absolutely want to have two or more types of security in place," she said.

When it comes to guarding against data breaches and preserving voice data privacy, companies should consider using voice-enabled systems that store the data directly on a device or locally, rather than in the cloud. "You are reducing your overall risk by retaining your audio" as opposed to allowing it to reside in the cloud, said Dr. Homayoon Beigi, president of Recognition Technologies and an adjunct professor at Columbia University. Like any other data, however, it is also important to retain only what is necessary.

"We shouldn't stop using this technology just because of some security threats. We should be cognizant of any threats and try the best we can to make these products secure."

The Voice Privacy Alliance, a nonprofit association of IT risk, cybersecurity and privacy experts, has also issued a set of guiding principles for addressing voice data privacy. The VPA advises entities to clearly and simply state the purpose of the collection of voice data, give consumers a choice regarding the use and sharing of this data, and allow them to opt-out at any point. Informed consent terms should always be written clearly and simply so that consumers understand the collection, use, security, sharing, retention and destruction practices for this data. The group also recommends that firms have accountable personnel overseeing data privacy and include voice data privacy monitoring in their routine governance, risk and compliance, and internal audit programs.

Even with such considerations, some experts remain skeptical that companies can adequately protect voice data. Picheny warned that, while today's customers usually have the option to delete their voice data, this may not always be the case as the technology becomes ubiquitous. "Will every major provider offer that ability?" he asked. Other experts simply advise against using voice technology in the first place. "Your best bet is not to use these devices or capabilities at all," Wenzler said. "At least not until we get to a point where the security structure is stronger and services become available that don't record everything."

Not everyone is so cautious, however. "We shouldn't stop using this technology just because of some security threats," said Damon McCoy, assistant professor of computer science at New York University's Tandon School of Engineering. "We should be cognizant of any threats and try the best we can to make these products secure."

Beyond passwords: Companies use fingerprints and digital behavior to ID employees

by Selena Larson @selenalarson

More companies are ditching passwords and using fingerprints and other biometrics to stop hackers.

"We're seeing a very rapid evolution from what used to be passwords, then smart cards, and now to biometrics," said Alex Simons, director of program management in Microsoft's identity division.

Biometric authentication uses face, fingerprint or iris scans to quickly confirm a person's identity. You probably already use itap by touching the home button to unlock your phone.

In the workplace, employees are increasingly using biometrics to log in to phones and computers, and to access data stored on those devices and in the cloud.

Spiceworks, a professional network for people in the IT industry, says nearly 90% of businesses will use biometric authentication by 2020, up from 62% today. Fingerprint scanning is currently the most common type of biometric authentication: 57% of organizations use it. Far fewer, just 14%, use facial recognition.

Companies such as Microsoft (MSFT) and Facebook (FB) are trying to get rid of passwords completely.

In 2015, Microsoft introduced Windows Hello with Windows 10. The new software uses face scans or fingerprints to log in to Windows devices. More than 50 million people use Windows Hello to log in to their PCs both in the home and at the office.

The Windows 10 Spring Creators Update will include a new authentication standard developed in collaboration with other tech companies, including Google. Called FIDO 2.0, the standard will enable Windows consumers to use multiple devices — including third-party security keys or a security monitors

that track your heart rate — to automatically log in to their computers without a password.

Related: Google's face match feature doesn't work in Illinois and Texas

"Passwords are the weak link. They have terrible characteristics about them, and they're hard for you to keep track of," Simons said. "Passwords are also super expensive for companies."

At Microsoft, Simons said he spends over $2 million in help desk calls a month helping people change their passwords.

Passwords are still widely used, of course, and one benefit is that they're easy to change if they're stolen. But you can't change your face or fingerprints, and biometrics can be stolen, too. In 2015, a breach at the federal Office of Personnel Management leaked 5.6 million people's fingerprints.

It's unclear for now what hackers can do with fingerprints. Experts worry that if they're adopted widely for authentication, it could lead to widespread identity theft. Researchers have already shown it's possible to use spoofed fingerprints to log in to smartphones.

Researchers have already tricked facial recognition by using a photo on older Windows devices and a Samsung smartphone.

Companies and consumers are also worried about third parties that are getting access to people's face scans through products like the iPhone X. Last year, Apple introduced facial recognition unlocking technology on the iPhone X and privacy advocates cited concerns about third-party companies having access to people's face scans. But the data shared with iOS developers reportedly can't unlock phones.

Meanwhile, Simons said biometrics collected with Windows are stored on the device directly and not shared to the cloud or with other third-party companies. Microsoft also provides the option to use a pin number instead of a biometric scan for anyone who is wary of sharing physical attributes.

State laws restricting biometric collection have hindered face and fingerprint-scanning tools or apps in some states. In 2008, Illinois passed a law that requires companies to let users know when biometric identifiers are collected

and how they will be used. It's also necessary to obtain consent from users before collecting and storing that data. In 2009, Texas passed a similar law. Data protection regulations about to go into effect in the European Union will also require consent before processing biometric data.

Biometrics will probably become just one part of a broader security strategy, perhaps as a second-factor login in addition to a password. Spiceworks' data shows just 10% of information technology workers think biometrics are secure enough to be the only form of authentication.

Other companies are using employee behavior to detect hacks.

Security firm BioCatch provides tools for companies to learn employees' digital behavior and identify when an unauthorized person is trying to access information.

Companies can add BioCatch software to apps and websites. It runs in the background to build a "behavior profile" of a user, and learns activities like how someone holds the phone, whether they type with one or two hands, and how they scroll or toggle between screens.

"The connected economy is forcing a need to redefine digital identity and to rely on new ways to make sure people are who they claim to be," said Frances Zelazny, vice president at BioCatch. "Your name and your pet's name, knowing that does not guarantee you really are a legitimate person."

Banks and the financial services industry are most interested in behavioral biometric technology. The Royal Bank of Scotland uses BioCatch.

People may be cautious about having their behavior tracked, but the trend toward biometrics should only grow.

"As we get better at explaining to the world how it works and as refine the software to make it easier to setup and use, more people are using it," Simons said. "Rather than trying to convince people that we're right, we're trying to give people options. We are trying to do everything in an upstanding manner to protect your privacy."

CNNMoney (San Francisco)First published March 18, 2018: 12:08 PM ET

Lizzie Kubitz

From: Noah Williams <noahsbwilliams@gmail.com>
Sent: Tuesday, February 06, 2018 8:09 AM
To: Rep. Matt Claman
Subject: Biometric Privacy Bill specifics

Representative Claman,

In principle I support your bill to safegard the personal data of Alaskans-but I feel it needs a provision of corcing cellular carriers to offer users a complete opt-out of all geolocation data services. The physical way in which cell phones are designed allows carriers practically unlimited access to devices (learn more about this here), so giving consumers both full transparancy and the capacity to opt-out of location data collection is essential. This is especially true in many areas of Alaska where one cellular carrier (GCI or AT&T) owns a complete monopoly over the cellular infrastructure and/or services.

Thank you for standing up for our rights

Be well,
—Noah Williams
(907)465-7291
District 33

INTERNET COALITION

NetChoice

Internet Association

CompTIA The IT Industry Trade Association

TECHNET THE VOICE OF THE INNOVATION ECONOMY

STATE PRIVACY AND SECURITY COALITION

February 20, 2018

Honorable Matt Claman, Chair
House Judiciary Committee
Alaska State Capitol
Room 118
Juneau, AK 99801

Re: HB 328, The Biometric/Geolocation Information Bill

Dear Chairman Claman:

The undersigned associations represent hundreds of the country's leading technology companies in high-tech manufacturing, computer networking and information technology, clean energy, life sciences, Internet media, ecommerce, education, and sharing economy sectors. Our member companies are committed to advancing public policies and private sector initiatives that make the U.S. the most innovative country in the world.

Biometrics and geolocation are new and exciting fields, offering consumers easy access to payment mechanisms, organization tools, hands-free activation technologies and valuable location-based services and features, and much more.

We urge you not to advance HB 328, your bill related to biometric and geolocation information. We are concerned that it is too broadly worded, could unintentionally hamper user experiences with burdensome notice and consent requirements, would disrupt many harmless conveniences that users have come to expect online, is unnecessary and offers no real or effective consumer protections.

We understand that it is challenging to regulate such complex areas in a balanced way while still allowing for innovation to flourish and protecting consumers from harm. We believe as drafted, this bill would create a categorical ban on private entities receiving biometric or location information from a device without forcing industry to put users through a burdensome consent process. Precise biometric and geolocation information that is linked to a specific individual should be treated appropriately, but since companies would have to obtain consent for the many positive and innocuous uses of biometric and location-based data under this bill, it would force companies to flood consumers mailboxes and mobile devices with annoying, disruptive and likely useless notices and consent requests.

That would impact a multitude of valuable and widely used services including "find my device" features and most applications involving photographs, free public wifi and mapping/navigation services. Other services that help people organize or make their lives easier could be disrupted or essentially banned by this bill, including products and services designed to provide critical services to those with developmental or physical disabilities. For example, someone that is hearing-impaired may rely on voice-recognition technology to stay independent, mobile, working or effectively communicating with others. Thousands of geolocation-based business models would be disrupted and/or limited such as valuable ridesharing, education, tourism, urban planning and telework applications.

Location controls are already strong, and most major mobile apps have privacy policies that users can view before and during their use of the service as well as device location controls regarding what apps can collect location information and what information they can collect. These policies are enforceable by the Attorney General and the Federal Trade Commission.

Since HB 328 contains broad and problematic definitions, would interrupt consumers' online experiences, is unnecessary, and would hinder businesses and deter innovation, we ask that you please not advance it.

Instead, we invite you to work with industry to craft a well-thought out, narrowly defined biometric and geolocation law that would adequately solve a specific issue, provide remedies in an effective way but one that is flexible enough to allow for innovation to flourish and avoids limiting an entire segment of data.

Sincerely,

Internet Coalition
Internet Association
CompTIA
State Privacy & Security Coalition
TechNet
Netchoice

cc: House Judiciary Committee members

March 21, 2018

The Honorable Matt Claman, Chair
House Judiciary Committee
Alaska State House of Representatives
State Capitol
Juneau, AK 99801

Sent by email: Representative.Matt.Claman@akleg.gov

Re: Protecting Alaskans' Privacy: ACLU of Alaska Support for HB 328

Dear Chair Claman, Vice-Chair Kreiss-Tomkins, and Members of the House Judiciary Committee:

The ACLU of Alaska supports House Bill 328. Ongoing technological developments enable private entities to obtain Americans' increasingly precise geolocational information and biometric data, such as fingerprints and facial scans. Without the right protections in place, private entities can access this data with disturbing ease and use it for commercial purposes. With the breaking news about Cambridge Analytica and the revelation that people could consent to release not just their own data, but the private personal data of all of their Facebook friends as well, makes privacy protections like these all the more important.[1]

And much of this private data is vulnerable to hacking. For example, the Samsung Galaxy S8 allows users to unlock their cell phone by scanning their iris, a biometric identifier that would be protected in HB 328. But hackers have already broken Samsung's iris recognition software.[2] And databases storing log in information are hacked regularly,[3] leading to identity theft.[4] Unlike passwords, which are easily changed, people can't change biometric identifiers like their fingerprints or irises.

---

[1] Matthew Rosenberg & Sheera Frenkel, *Facebook's Role in Data Misuse Sets Off Storms on Two Continents*, NEW YORK TIMES (Mar. 18, 2018) https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html.

[2] Dan Goodin, *Breaking the iris scanner locking Samsung's Galaxy S8 is laughably easy*, ARS TECHNICA (May 23, 2017) https://arstechnica.com/information-technology/2017/05/breaking-the-iris-scanner-locking-samsungs-galaxy-s8-is-laughably-easy/.

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

[4] *Identity Theft*, https://www.usa.gov/identity-theft.

Without notice and consent, people will not know how their own private information is collected, who can access it, and how it is used.

HB 328 works to combat these threats to Alaskans' privacy: it provides valuable protections for Alaskans that will require private entities that collect geolocational and biometric data to inform Alaskans that their private information is being collected and will require consent before collecting it.

But Facebook and other companies are trying to kill this bill.[5] Facebook works through CompTIA, an industry group, to defeat bills that would give users more control over how their likenesses are used or whom they are sold to.[6] In 2016 alone, Facebook spent over $9.3 million in its lobbying efforts nationally.[7] Facebook developed an inhouse facial recognition project, DeepFace, which has access to photos of 2 billion monthly users and all the friends in photos they upload. Essentially, according to a DeepFace engineer, this is "a system that could recognize the entire population of Earth."[8] Without regulations in place, Facebook can do whatever it wants with this data without telling its users.

We appreciate the opportunity to testify about HB 328 with the House Judiciary Committee and urge the Committee to support this bill. It would allow Alaskans to preserve the privacy they rely on, even as informational technology continues to advance and potentially encroach deeper into people's private lives.

Sincerely,

Melissa H. Goldstein
Legal Fellow

cc: Vice Chair Kreiss-Tomkins, Representative.Jonathan.Kreiss-Tomkins@akleg.gov
Representative Stutes, Representative.Louise.Stutes@akleg.gov
Representative LeDoux, Representative.Gabrielle.LeDoux@akleg.gov
Representative Eastman, Representative.David.Eastman@akleg.gov
Representative Kopp, Representative.Chuck.Kopp@akeg.gov
Representative Reinbold, Representative.Lora.Reinbold@akleg.gov
Representative Millett, Representative.Charisse.Millett@akleg.gov
Representative Zulkosky, Representative.Tiffany.Zulkosky@akleg.gov

---

[5] Jared Bennett, *Facebook: Your Face Belongs to Us*, THE DAILY BEAST (July 17, 2017) https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.

[6] *Id.*

[7] *Id.*

[8] *Id.*

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.