

Chair David C. Farnsworth
Transportation and Technology Committee
Arizona State Senate

February 3, 2023

RE: Opposition to SB 1238 - Concerning biometric information

Dear Chair Farnsworth and members of the committee,

While well intentioned, we ask that you not advance SB 1238 as it has fundamental flaws that will undermine Arizona citizens' ability to use amazing services available to your neighboring states.

Just the other day I built a photo album using facial recognition features provided by Shutterfly and used my DoorCam to identify when my family got home safely. But passing SB 1238 would deny Arizona residents such tools.

The growing use of biometrics brings with it significant concerns about consumer privacy and security. Fortunately, there are already mechanisms in place to appropriately regulate the industry. Thus, we agree with the Federal Trade Commission's (FTC) conclusion in their 2015 *Internet of Things* Report that "there is great potential for innovation in this area, and that [] specific legislation at this stage would be premature."¹

There are numerous positive uses of biometrics that SB 1238 will curtail. And we've already seen the negative results of overly aggressive laws and regulations.

Illinois went down the wrong path on biometric privacy to the detriment of its citizens.

[B]etween 2015 and 2020 alone, there were over 1,000 Illinois BIPA class action complaints filed across the United States, with additional new filings continuing to be initiated every day.²

The Illinois Biometric Privacy Act (BIPA) has been abused by class-action lawyers seeking big payouts for otherwise beneficial uses of biometric data. BIPA was abused to sue the photo printing company Shutterfly. Shutterfly allowed customers to use facial recognition on the customer's own photos to find pictures of specific friends and family – a violation of the overly restrictive BIPA. Shutterfly settled with a class-action lawfirm³ but left the people of Illinois without facial searching of their own photos.

¹ Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* at vii (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (2015 FTC IOT Report)

² *Employers Take Note – New York Introduces A Biometric Information Privacy Bill Identical To The Illinois BIPA*, JCSupra, (Jan. 11, 2021)

³ Ally Marotti, *Shutterfly lawsuit tags Illinois as battleground in facial recognition fight*, Chicago Tribune (Sept. 21, 2017)

Likewise, as a result of the BIPA, Illinois residents no longer have access to services like facial recognition on Amazon Photos or the ability to identify friends and family on Nest Cameras. But it doesn't just stop with commercial services. When Artists perform in Illinois, the Artists can't use facial recognition to identify stalkers at concerts creating real safety concerns.

The screenshot shows the Amazon Help & Customer Service page. The main heading is "Notice to Illinois Residents". The page content includes:

- A breadcrumb trail: Digital Music, Amazon Video & Apps > Prime Photos & Amazon Drive > Prime Photos Features & Apps >
- A search bar with "Search Help" and a "Go" button.
- A left sidebar with "All Help Topics" and a list of topics under "Prime Photos Features & Apps":
 - About Prime Photos Features
 - Search and Organize your Photos with Prime Photos
 - Managing Family Vault Members
 - Managing Photos in Family Vault
 - Notice to Illinois Residents**
 - Upload a Photo or Video Using the Prime Photos Website
- A "Quick solutions" section with icons and links for:
 - Prime Video: Manage preferences & settings
 - Apps & Devices: Install or remove apps
 - Digital Purchases: View purchased books & apps
 - Manage Your Music: Upload music & edit playlists
- Main text:
 - Image recognition features are disabled initially for Illinois residents because an Illinois state law may require the informed written consent from an Illinois resident before performing image recognition on photos that include his or her face.**
 - Enabling Image Recognition on Photos.** By enabling image recognition features for your account, you understand that image recognition analysis will be performed on the photos stored in your account, and you represent to us that you have obtained the consent of the individuals in the photos stored in your account permitting us to use image recognition analysis on photos of them.
 - Image Recognition on Photos in Family Vault.** The user who established a Family Vault controls whether image recognition features are enabled in the Family Vault. If you enable image recognition features in your Family Vault, you understand that image recognition analysis will be performed on the photos stored by each member of the Family Vault, and you represent to us that you have obtained the consent of each member of your Family Vault to use image recognition analysis on photos of them. Further, you represent that you have ensured that each member of your Family Vault has obtained the consent of the individuals in the photos they store with us to use image recognition analysis on photos of them.
 - If you are invited to participate in a Prime member's Family Vault, the Prime member who invited you will control whether image recognition features are enabled for the Family Vault. If the image recognition features are enabled for the Family Vault, image recognition analysis will be performed on the photos you store with us. By accepting the Family Vault invitation, you represent to us that you have obtained the consent of each individual in your photos to use image recognition analysis on photos of them.
 - You may access the image recognition features by navigating the setting page in your Prime Photo account.

Because of BIPA, Amazon Photos does not allow searching photos by face for Illinois residents

Fingerprint taken for Six Flags season pass could clear way for class-action lawsuit

Published: Jan. 25, 2019 at 4:01 p.m. ET

By [Andrew Keshner](#)

Because of BIPA, Six Flags in Gurnee, Ill was sued over allowing season ticket holders to use fingerprints for verification



State-of-the-art smart.

Nest Cam IQ has serious processing power, so it can do things like tell a person from a thing. And even recognize faces with Nest Aware.*

[Add familiar face alerts* >](#)
with Nest Aware subscription

- 6-core processor
- Better connectivity†
- Person alerts

*Familiar face alerts require a Nest Aware subscription. Not available on Nest Cams used in Illinois.
†Compared to Nest Cam Indoor, thanks to 802.11ac Wi-Fi and a 2x2 MIMO chip.

Because of BIPA, Nest does not allow Illinois residents the ability to identify friends and family members



Because of BIPA, restaurant kiosks allowing quick reorder of meals at Wao Bao via customer recognition are no longer available in Illinois

State Journal Register - *Innovation for America – but not for Illinois*, by Steve DelBianco

[The Illinois Biometric Privacy Act (BIPA)] — legislation designed to protect personally-identifiable information such as fingerprints, retina scans, and facial images. Over the past couple of years, these same class-action attorneys have abused these laws to increase their bottom line while harming some of our country’s leading tech companies. They shook down the photo website Shutterfly for letting users search their own photos with facial recognition tools to find that perfect photo of their spouses and pets. They even recently filed suit against the restaurant Wow Bao whose self-order kiosks allow users to opt-in to facial recognition for faster future orders.

These are services that are supposed to be convenient for users and inspire innovation, but that’s not what’s happening here. Instead we find these specialized law firms deceiving the industry to line their own pockets with the profits from these frivolous lawsuits.

It wasn’t enough to stop us from tagging family members in our own photos. During this year’s spring legislative session, these class-action lawyers pushed for bills promoted as “pro-privacy” and “pro-consumer” that they claim would be good for Illinois residents, but were really just pro-lawsuit.⁴

Fortunately, numerous federal and state laws are already in place to protect the privacy and secure the data of Arizona consumers. These include the Children’s Online Privacy Protection Act (COPPA), the Electronic Communications Privacy Act (ECPA), the state’s Data Breach Notification and Consumer Protection laws, and common law legal doctrines protecting privacy and data security.

Moreover, privacy protections regarding biometrics already exist and are enforced robustly by the Federal Trade Commission (FTC). The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices.

This framework is the ideal way to regulate biometrics, as the FTC’s technology-neutral case-by-case approach has proven an effective way to ensure companies implement strong data security and privacy protections without stifling innovation. Relying on Section 5’s “unfair or deceptive practices” clause and providing guidance through enforcement, the FTC’s approach allows it to adjust its enforcement approach as technology evolves and industry best practices change.

We agree with the FTC’s recommendation that “companies should build security into their devices at the outset, rather than as an afterthought,”⁵ by implementing a security by design process. An example of this so-called security by design principle in practice is the increased use of encryption technology by businesses consistent with FTC guidance.⁶

⁴ Steve DelBianco, *Innovation for America – but not for Illinois*, State Journal Register (Oct. 24, 2017).

⁵ Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* at 44 (2015).

⁶ Federal Trade Commission, *Start with Security: A Guide for Business* (2015), <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

Further, the FTC's 2012 Privacy Report recommended industry best practices for protecting the privacy of consumer data.⁷ Companies should follow the FTC's guidance on both security by design and privacy best practices in designing their products to protect their customers' information, or else they could find themselves in violation of Section 5 and bereft of their customers' trust.

We appreciate your thoughtful consideration of our concerns. For the reasons outlined in this letter, we urge against moving SB 1238 due to its unintended consequences.

We welcome the opportunity to work with this committee more as it considers the ideal approach for the citizens of Arizona.

Sincerely,

Carl Szabo

Vice President and General Counsel, NetChoice

NetChoice is a trade association that works to make the internet safe for free enterprise and free expression. www.netchoice.org

⁷ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (2012 FTC Privacy Report).