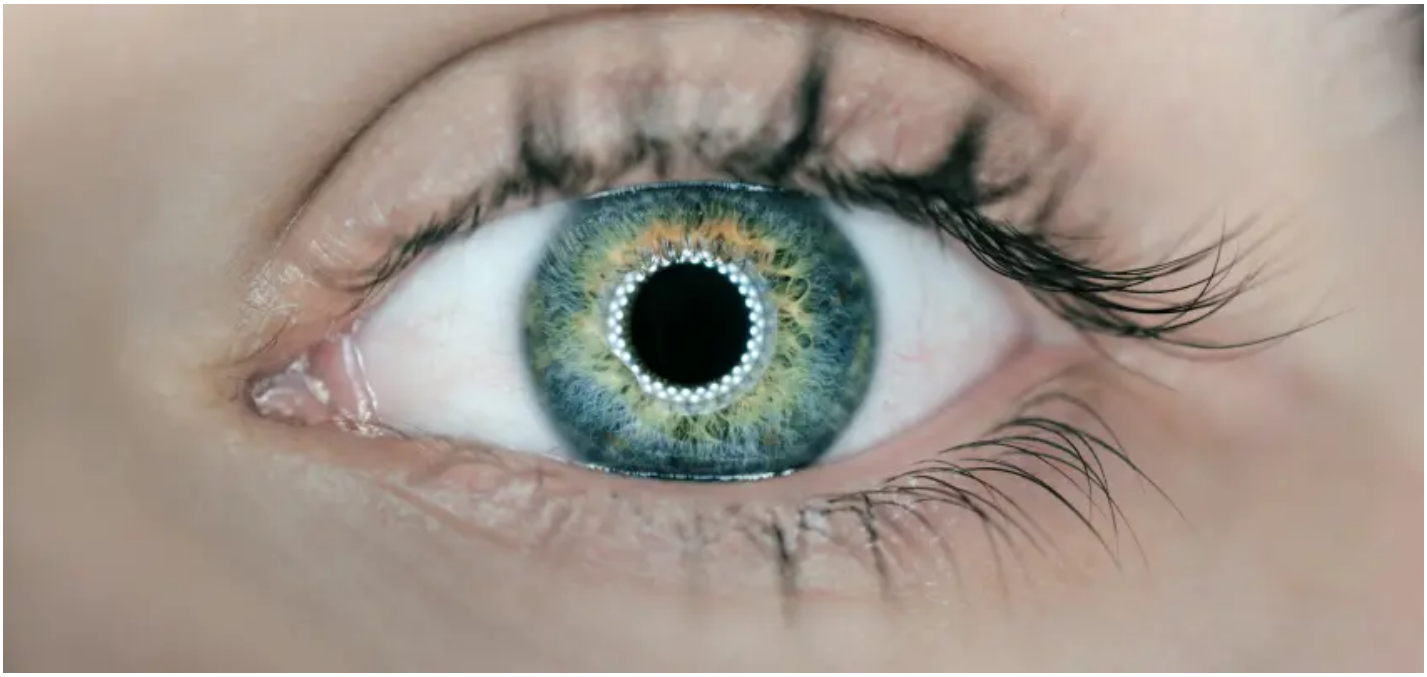
11-23-2021

Biometric Data Collection: Market Necessity or Unconstitutional Overkill?

Thomas Langtry

GGU Law Review Blog



NOVEMBER 23, 2021 NO COMMENTS

Biometric Data Collection: Market Necessity or Unconstitutional Overkill?

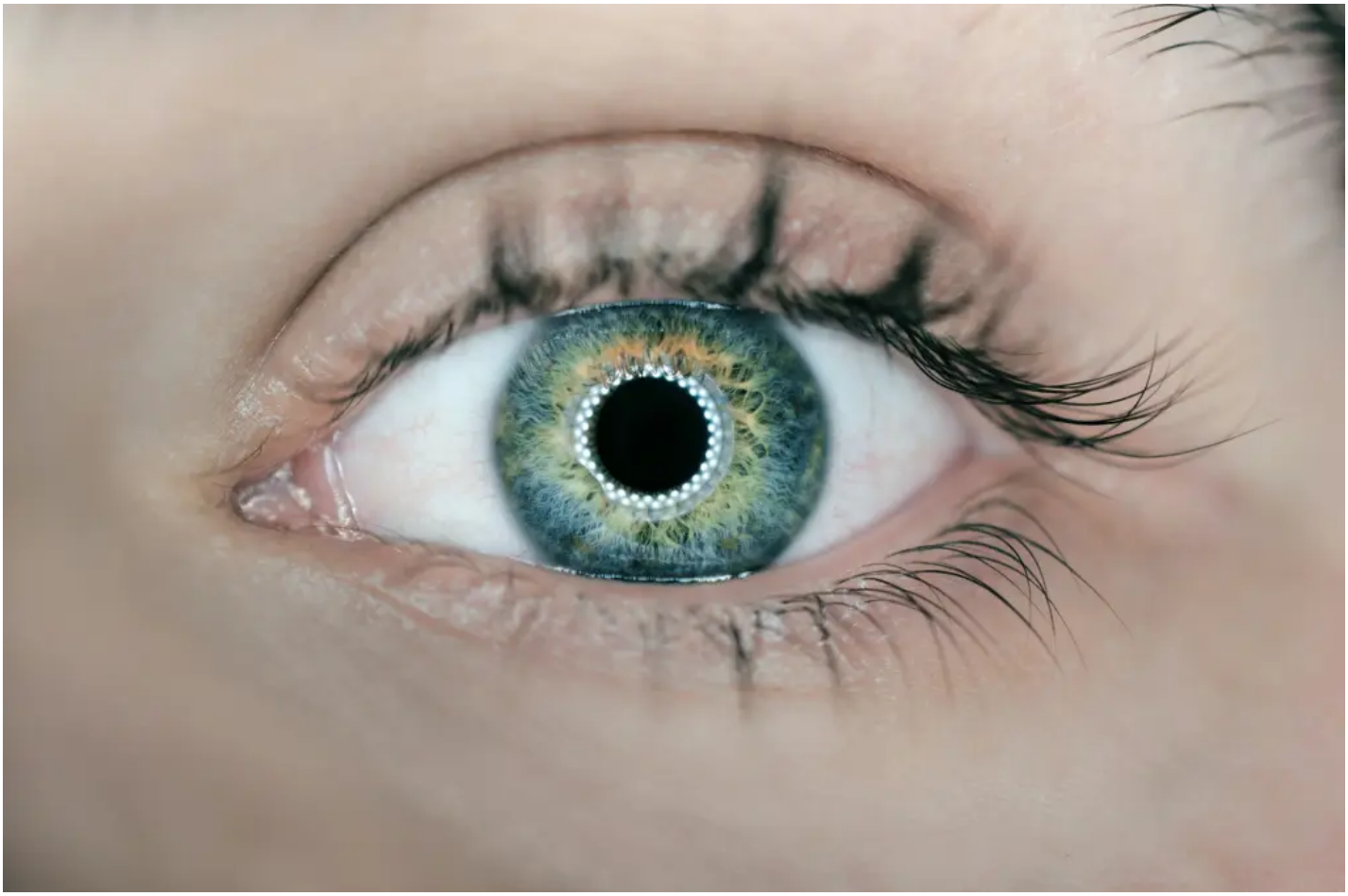


Photo by Arteum.ro on Unsplash

Congress should pass, and the President should sign into law, the National Biometric Information Privacy Act of 2020 (National BIPA). Introduced by Senators Jeff Merkley (D-OR) and Bernie Sanders (I-VT), this bill limits the ability of private entities to collect biometric data and requires them to ensure the privacy and security of data they do collect. Unlike most federal regulatory legislation, it also provides for a private right of action through which individuals can seek meaningful remedies.

Critics argue that the bill will deprive consumers of online shopping services and convenient digital security, and that employers and retailers may retaliate by requiring consent for biometric data collection as a condition of service or employment. Supporters argue that the status quo has already defaulted to mandatory consent, and that without legislation, citizens who value their privacy are left without a remedy.

Biometric data collection provides relatively negligible benefits in commercial and employment contexts. Conversely, unregulated collection erodes civil liberties and violates the fundamental right to privacy. On balance, the risks far outweigh the benefits.

What Is Biometric Data?

Biometric information is distinguishable from personal information. According to the California Consumer Privacy Act of 2018 (CCPA), personal information relates to the identity of consumers or households. Examples include names, signatures, social security numbers, addresses, telephone numbers, passport and driver's license information,

bank account numbers, and medical information. Personal information excludes information lawfully available to the public through federal, state, or local government records.

By contrast, biometric information includes intimate behavioral, physiological, and biological data, such as deoxyribonucleic acid (DNA); imagery of the iris or retina; fingerprints; face, hand, palm, and vein patterns; voice recordings; keystroke or gait patterns; and sleep, health, or exercise data.

Who Wants My Biometric Data?

Financial institutions and healthcare organizations frequently collect biometric data. Banks collect information to prevent fraud. Healthcare providers cite the need to protect the security of routinely gathered biological information as justification for using biometric data collection technology. Indeed, Section 5 of the National BIPA carves out exceptions for these industries by requiring agreement with the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.

Other uses of biometric data are more controversial. Eversheds Sutherland, LLP is an international law firm that defends businesses in consumer class actions. In a 2020 whitepaper, Eversheds Sutherland Partner Frank Nolan acknowledged that recent growth of biometric technology has outpaced the law. Unprecedented innovations in the Internet of Things (IoT), artificial intelligence (AI), and edge computing have made commonplace the presence of biometric data collection technology in homes and businesses. In fact, most people have already provided biometric information to a private entity.

According to Nolan, these new technologies are valuable because they enable auto-unlock features on digital phones and secure access to bank accounts and work areas using fingerprints or facial recognition scans. Biometric data collection also helps organizations understand where and when people gain access to commercial and residential property. Thus, this triggers for businesses enticed by the potential for surveillance and information control the need to confront practical and legal questions about biometric data retention, security, and destruction.

Finally, many businesses engage in overtly commercial exploitation of biometric data. Writing in the Kansas Law Review, Hannah Zimmerman cites research in which electroencephalogram (EEG) headsets measured responses to stimuli like food and celebrities, with the resulting “brainprints” identifying individuals with 100% accuracy. Increasingly, private industries surreptitiously collect and sell vast amounts of biometric data, including people’s physical locations, websites they visit, personal associations, religious and sexual preferences, and marital and financial statuses. Marketing companies use these invasive data collection techniques to generate massive profits through engineered website user experiences and advertising campaigns.

Objections to Biometric Data Collection

Photo by Matthew Henry on Unsplash.

The primary objection to biometric data collection is singular but profound. Although support for the continued growth of this industry is widespread, its sheer volume and increasing omnipresence pose grave concerns that the National BIPA can begin to address. Experts agree that overcollection of biometric data fuels the loss of intellectual privacy, which in turn stifles society's ability to develop ideologically and artistically. The freedom resulting from the presumption of public anonymity disappears when we are forced to live with the knowledge of ongoing, systematic public observation. The Constitutional right to privacy, to which Justices Warren and Brandeis referred in 1890 as the "right 'to be let alone,'" militates against a fishbowl society characterized by constant surveillance.

Current State of the Law

Photo by Vlad Tchompalov on Unsplash

The Privacy Act of 1974 prohibits federal agencies from disclosing private records without written consent. The Privacy Act defines "record" broadly to include any individually identifying data, such as names, numbers, symbols, and even fingerprints, voice prints, or photographs. However, it fails to address recent developments in biometric technology or the information collection practices of private entities.

In response, many states have enacted statutes specifically addressing private-sector biometric information collection. In California, Section 1798.140 of the CCPA's broad definition of personal information includes a designation for biometric information, rendering the law potentially useful as a tool to prosecute violations of biometric data collection regulations. However, only Illinois, Texas, and Washington have enacted standalone legislation. Although none of these laws prohibit biometric data collection *per se*, they mandate varying degrees of notice.

The Illinois Biometric Information Privacy Act (Illinois BIPA) has received the most attention and is the model for the National BIPA. The Illinois BIPA includes one consent requirement for collection, storage, and use and another for disclosure and dissemination. It prohibits companies from profiting from collection and use of biometric data and requires them to publish a schedule of data retention and destruction. Finally, it requires the exercise of a reasonable standard of care.

The Illinois BIPA, the most restrictive biometric privacy statute, is the only one to include a private right of action. Under the Illinois BIPA, plaintiffs can claim the greater of $1,000 in liquidated or actual damages for negligent violations; the greater of $5,000 in liquidated or actual damages for intentional or reckless violations; liquidated damages for reasonable attorneys' fees and costs; and injunctive relief.

Many Illinois residents have successfully filed individual and class actions, the majority of them citing violations of the consent requirement for collection, storage, and use. Typically, companies remove to federal court and offer procedural defenses, most frequently by attacking plaintiffs' ability to show an injury-in-fact to establish Article III standing. Because the Illinois Constitution does not include a standing requirement, plaintiffs fare well in Illinois state courts. Pro-plaintiff decisions in the District Court for the Northern District of Illinois and the Ninth Circuit have also begun to chip away at the standing defense.

Less frequently, out-of-state employers may argue lack of personal jurisdiction. Other, more case-specific means of defending against consumer actions include Constitutional defenses like preemption by federal statute, violations of the Dormant Commerce Clause, and extraterritoriality. Significantly, none of these defenses attack the substantive arguments of plaintiffs.

Regulation under the National BIPA

The National BIPA mirrors the Illinois BIPA's consumer-friendly approach. Section 3 mandates specific methods for data collection, retention, disclosure, and destruction. Section 4 provides an individual right of action under which violations of Section 3 constitute an injury-in-fact, thereby precluding the Constitutional standing defense.

Remedies include the greater of $1,000 in liquidated or actual damages per negligent violation; the greater of $5,000 in liquidated or actual damages per intentional or reckless violation; discretionary punitive damages not to exceed $5,000 per violation; reasonable attorneys' fees and costs; injunctive relief; and specific performance requiring permanent data destruction.

Critics of the National BIPA cite expensive decisions like the claim against the Trump hotel chain, in which employees sued after they were required to submit their fingerprints to facilitate time-tracking. Critics also argue that developing policies to avoid similar cases is burdensome to in-house counsel, and that the National BIPA will arm money-motivated consumers and consumer advocacy law firms with a litigation weapon similar to the Fair Debt Collection Practices Act (FDCPA) or the Telephone Consumer Protection Act (TCPA). Finally, critics warn that restricting biometric data collection will limit consumers' ability to auto-unlock digital phones, pass through automated security systems, or receive product advertisements tailored to their behavioral and genetic characteristics.

Supporters of the National BIPA argue that leveling the playing field between consumers and corporations is long overdue. Few would support a repeal of the FDCPA or the TCPA and a return to the age of abusive debt collectors and telemarketers. Consumers who must have auto-unlock features on digital phones can provide written consent for biometric data collection. Finally, although the National BIPA limits retailers' ability to surreptitiously collect intimate private details about potential customers, the advertising industry will not likely suffer any materially adverse injury.

The marginal benefits of biometric data collection do not outweigh the unprecedented and profound risks. Special interests cannot limit Congress's power to defend the rights of American citizens. The urgency with which Congress should pass the National Biometric Information Privacy Act cannot be overstated.

Email Twitter Facebook LinkedIn

Like this:

Like

Be the first to like this.

Thomas Langtry

Thomas Langtry is a J.D. Candidate at Golden Gate University School of Law, Class of 2024; Staff Writer, Golden Gate University Law Review; Events Coordinator, International Law Society; 1L Student Representative, Westlaw-Thomson Reuters; and Executive Committee Member, Bay Area Young Tax Lawyers.

Leave a Reply

Enter your comment here...

Search blog

Search

Archive

Select Month