BLANKROME

Cybersecurity & Data Privacy

AUGUST 13, 2020 • NO. 14

U.S. Senators Introduce Bill Imposing Stringent, National Biometric Privacy Regulation

Biometric data—like fingerprints and facial geometry scans—allows companies across all industries to significantly enhance their operations in a myriad of ways. At the same time, the call for regulation over this especially sensitive type of personal data continues to grow. On August 4, 2020, U.S. Senators Jeff Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act of 2020 (the "Act"). If enacted, the Act would impose uniform, draconian requirements closely mirroring the Illinois Biometric Information Privacy Act ("BIPA")—which has led to massive, plaintiff-driven litigation—across all 50 states.

While it is unknown whether this bill will ultimately become law, the Act highlights the need for all companies using biometric data—regardless of where they are located—to take proactive measures to implement flexible, adaptable biometric privacy compliance programs.

OVERVIEW OF BIOMETRIC DATA

Biometric data generally encompasses unique, measurable human biological or behavioral characteristics—including fingerprints, voiceprints, and scans of hand or face geometry—for identification and authentication purposes. Importantly, biometric data is different from Social Security numbers and other forms of personally identifiable information ("PII") that are unique to specific individuals. Once compromised, biometric data has forever lost its ability to be used as a secure identifying mechanism.

APPLICABILITY

One of the more significant aspects of the Act pertains to its essentially unlimited scope. The Act would apply to "private entities"—which is defined as "any individual, partnership, corporation, limited liability company, association, or other group, however organized." Thus, unlike some other recently-enacted privacy laws—like the California Consumer Privacy Act of 2018 ("CCPA")—the Act would not be limited by any preliminary thresholds for entities to fall under the scope of the law, such as total gross revenue.

CORE REQUIREMENTS SIMILAR TO ILLINOIS BIOMETRIC PRIVACY ACT ("BIPA")

Under the Act, covered entities would be subject to many of the same requirements and restrictions mandated by Illinois' biometric privacy law:

- **Public Policy:** Covered entities must maintain a publicly available biometrics privacy policy that includes, at a minimum, a retention schedule and guidelines for permanently destroying biometric data within mandated timeframes.
- **Written Notice:** Before collecting or using an individual's biometric data, covered entities must provide the individual with written notice detailing the entity's biometric practices and its use of the individual's biometric identifiers.
- **Written Release for Initial Collection/Use:** Before collecting or using an individual's biometric data, covered entities must obtain a written release from the individual authorizing such collection or use.
- **Written Release for Disclosures:** Similarly, a written release must be obtained from an individual before disclosing that individual's biometric data to any third party.
- **Prohibition on Selling, Leasing, or Otherwise Profiting from Biometric Data:** The Act bars covered entities from selling, leasing, trading, or otherwise profiting from the use of biometric data.
- **Reasonable Security Measures:** Covered entities must safeguard biometric data from unauthorized access, disclosure, or acquisition: (1) using the reasonable standard of care applicable to the entity's given industry; and (2) in a manner that is the same or more protective than the manner used by the entity to safeguard other types of sensitive personal data.

ADDITIONAL REQUIREMENTS BEYOND BIPA

In addition, the Act also contains several additional requirements not found in BIPA:

- **Purpose Requirement:** Covered entities are prohibited from collecting or otherwise obtaining individuals' biometric data unless the entity requires such data to provide a service, or for some other valid "business purpose" (which is not defined in the Act).
- **Right to Know:** The Act also contains a "right to know" similar to that contained in the CCPA, which requires covered entities—upon request—to disclose information regarding the biometric data the entity has collected, where the data originated, the use(s) of the data, and whether and to whom the data is being disclosed or sold.
- **Prohibition on Use of Biometric Data for Advertising Purposes:** In addition to prohibiting the sale of, or otherwise profiting from, the use of biometric data, the Act also bars the use of biometric data for advertising purposes as well.

PENALTIES & ENFORCEMENT

Also similar to BIPA is the Act's primary enforcement mechanism, which entails a private right of action permitting any "aggrieved individual" to pursue litigation against an entity that fails to comply with the Act. Consumers can pursue individual or class lawsuits and can recover up to $1,000 in liquidated damages for each negligent violation, and actual damages and any punitive damages awarded up to $5,000 for each intentional or reckless violation.

Critically, the Act also features a unique provision that "[a]ny such violation constitutes an injury-in-fact and a harm to any affected individual"—which would allow plaintiffs to completely avoid any potential statutory standing hurdles that often serve as roadblocks in similar litigation, as the law explicitly specifies that individuals possess standing to sue for any violations of the law. In addition, the Act also enables state attorneys general to bring suit on behalf of their residents as well.

KEY TAKEAWAYS

The Act in the very early stages of the legislative process and will likely face fairly stringent opposition from both the tech industry and a number of Senators, especially as it relates to how the law should be enforced and, more specifically, whether a federal law of this nature should provide a private right of action for individuals to pursue litigation directly against covered entities.

Ultimately, however, even if the Act fails to make its way into law, it is clear the scope of potential liability exposure in connection with the use of biometric data will continue to increase rapidly in the immediate future. Companies should not wait for new regulation to be passed, but instead, should take preemptive action by enhancing their compliance programs to directly address biometric privacy This can be achieved by implementing the overarching privacy principles that are found in today's most stringent biometric privacy statutes and bills, including notice, consent, written releases, and biometric data security measures.

WHAT TO DO NOW

If your organization currently utilizes any type of biometric data—or if it is considering doing so in the future—the best course of action is to speak with experienced counsel to ensure your organization has the necessary policies, procedures, and practices to satisfy the full range of current and anticipated biometric regulatory compliance obligations, and to properly manage potential risk.

As leaders in the biometric privacy space, Blank Rome's *Biometric Privacy Team* can assist with providing key counseling and guidance regarding issues or concerns relating to the use of biometric data or today's new wave of biometric privacy laws. We can also assist in developing tailored, comprehensive biometric privacy compliance programs that ensure continued, ongoing compliance not just with current biometrics regulation, but anticipated laws as well—allowing you to stay a step ahead of today's constantly-evolving legal landscape.

For additional information, please contact:

Jeffrey N. Rosenthal, Philadelphia Office
Partner, Biometric Privacy | Cybersecurity & Data Privacy
Privacy Class Action Defense
215.569.5553 | rosenthal-j@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Biometric Privacy | Cybersecurity & Data Privacy | Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com