

## HR 4381

### Biometric Information Privacy Act

**Congress:** 113 (2013–2015, Ended)

**Chamber:** House

**Policy Area:** Civil Rights and Liberties, Minority Issues

**Introduced:** Apr 2, 2014

**Current Status:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

**Latest Action:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. (Apr 16, 2014)

**Official Text:** <https://www.congress.gov/bill/113th-congress/house-bill/4381>

### Sponsor

**Name:** Rep. Stockman, Steve [R-TX-36]

**Party:** Republican • **State:** TX • **Chamber:** House

### Cosponsors

No cosponsors are listed for this bill.

### Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	House	Referred to	Apr 16, 2014

### Subjects & Policy Tags

#### Policy Area:

Civil Rights and Liberties, Minority Issues

### Related Bills

No related bills are listed.

Biometric Information Privacy Act - Establishes an offense that subjects business entities (including organizations, trusts, and nonprofits), government entities, and people to penalties for knowingly: (1) obtaining in a fraudulent manner personal physiological biometric information relating to an individual, or (2) disclosing such information without permission from the individuals to whom the information pertains.

Defines "personal physiological biometric information" as genetic information, finger prints, palm prints, hand geometry, iris scans, retina scans, and eye vein scans.

Sets forth the following penalties to apply to such offenses:

- a fine of up to \$50,000, imprisonment for up to 1 year, or both;
- if the offense is committed under false pretenses, a fine of up to \$100,000, imprisonment for up to 5 years, or both; and
- if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of up to \$250,000, imprisonment for up to 10 years, or both.

Permits a governmental entity to obtain such personal information pursuant to a court order only if, in the court proceeding relevant to such order: (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case, and (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

Requires the Attorney General (DOJ) to enforce violations of this Act.

## **Actions Timeline**

---

- **Apr 16, 2014:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Apr 2, 2014:** Introduced in House
- **Apr 2, 2014:** Referred to the House Committee on the Judiciary.