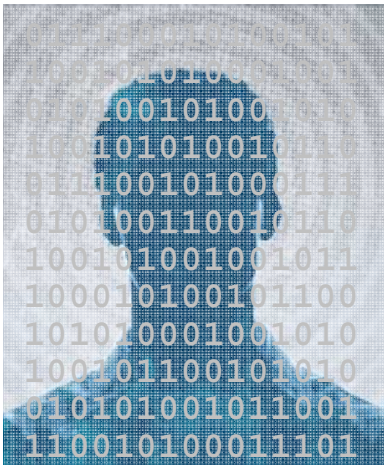
Privacy and Personal Data Protection Act

Sen. Harriette Chandler :: Rep. Jason Lewis



In recent years, the federal government has provided the states with enormous sums to build vast data-banking operations which collect and sift through a huge array of information about ordinary Americans.

There are more than 70 information super-hubs – "fusion centers" – set up across the country, with two right here in Massachusetts, operating under the auspices of the State Police and the Boston Police Department.

The U.S. Department of Homeland Security has explicitly stated that it's up to the states to provide privacy protection for these operations. The **Privacy and Personal Data Protection Act** *responds to that challenge.*

Protecting Political Activity

These data centers were originally established for the legitimate purpose of preventing terrorism. However, their missions and their operations have expanded dramatically and there are already numerous examples of abuse. Around the country, peaceful political organizations have been monitored and labeled as "terrorist" groups. In Virginia, it was historically Black colleges and universities. In Maryland, it was Amnesty International and an anti-death penalty coalition. In Missouri, it was Libertarian Party supporters. In California, environmental and labor union activism ended up in terrorism-related databases.

Massachusetts is the birthplace of constitutionally protected freedom of speech. We need to protect that freedom.

The **Privacy and Personal Data Protection Act** aims to protect our First Amendment rights and our personal data, while maintaining effective law enforcement functions.

Protecting Privacy and Personal Data

The statewide "Commonwealth Fusion Center" and the urban area "Boston Regional Intelligence Center" can access both government databanks and exhaustive private sector information compiled by private data-mining companies.

By collecting and sharing residents' personal information, we make a huge leap from simply investigating and responding to specific threats or crimes to examining data on ordinary Massachusetts residents, *even those not suspected of any crime*.

This data-gathering, banking, and sharing, goes far beyond the bounds of ordinary law enforcement investigations into criminal acts. Permitting government entities to rummage through and share residents' personal data from dozens of sources, not just from law enforcement – carries real risks.

The **Privacy and Personal Data Protection Act** would establish practical, sensible standards to ensure that government collection of our personal information is conducted in a secure, accountable manner, and would establish necessary transparency and oversight structures.

Bill Summary: **The *Privacy and Personal Data Protection Act***
S.1194/H.1336 **will make Massachusetts residents more secure**

Protects First Amendment rights

- Prohibits law enforcement collection of information about individuals' political and religious views, associations, or activities — *unless* it relates directly to a criminal investigation based on reasonable suspicion of criminal conduct.

Focuses law enforcement resources where they are most effective

- Reliable information and reasonable suspicion are the bases for effective investigations.
- Law enforcement will get better "hits" from a database that contains quality information. We can't afford to waste scarce resources profiling people based on diffuse information and conjecture.

Safeguards personal data from improper use by the government

- Currently, law enforcement is capable of collecting staggering quantities of personal information from for-profit data aggregating services, including:
    - property ownership and transfer records;
    - consumer credit, loan, lien, and bankruptcy information;
    - criminal and civil court records;
    - corporate filings and federal licensing information;
    - employment and residential histories;
    - Social Security and telephone numbers.
- This bill codifies standards from federal regulations in state law, establishes data security procedures, and ensures that information is reviewed and reliable.
- Trawling through personal information for possible hints about unspecified criminal activity is the wrong approach. This bill will prevent government databases from keeping such information unless it is used for investigations based on reasonable suspicion.

Creates transparency & oversight for data collection

- Establishes internal audits to ensure compliance with data security standards.
- Creates independent oversight and public reporting by the Inspector General.
- Clarifies that the Fair Information Practices Act applies to these data centers so that an individual can find out what information is kept about him or her, with exceptions for criminal investigations, confidential sources, and others' privacy and safety.

It's Time to Take the Next Step

In recent years, Massachusetts has protected people's personal information from identity theft and overhauled the CORI system to ensure that information is accurate and used appropriately.

Now it's time to ensure the proper use of information about MA residents in another context – the expanding government operations that are collecting and sharing residents' personal information.