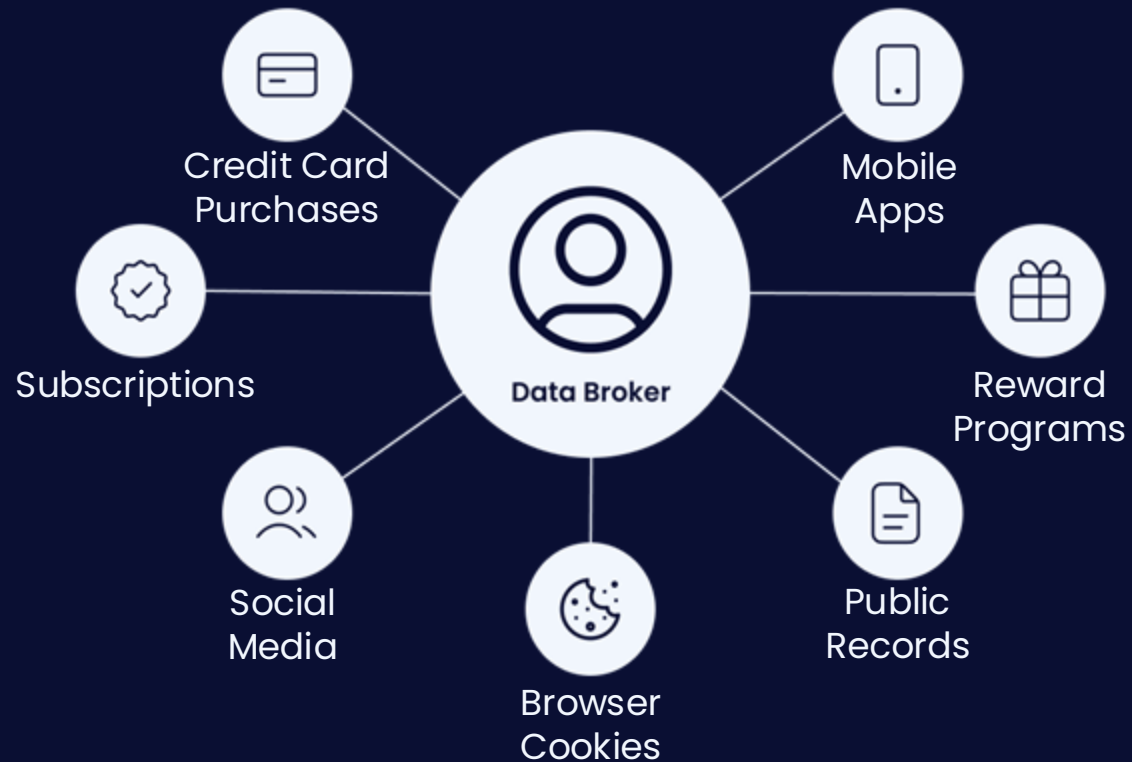NCSL Task Force on Artificial Intelligence, Cybersecurity and Privacy

$350B Industry

Data Brokers are collecting and exposing, and selling your data online

- Credit Card Purchases
- Mobile Apps
- Subscriptions
- Reward Programs
- Social Media
- Public Records
- Browser Cookies
- Data Broker

NCSL
CELEBRATING 50 YEARS

FamilyTreeNow.com

Individual and Organizational Risk

Why you, Why now?

89%
State legislators

52%
Local officeholders
Experiencing threats or attacks within the past three years

[Brennan Center for Justice](#)

87%
Local officials reported a rise in attacks

81%
Said they had personally experienced harassment, threats, or physical violence

[The National League of Cities (NLC)](#)

400%
Increase in **Judges'** threats

4,000
Incidents, over the last five years, many of them death threats sometimes ending in violence

[Tennessee Bar Association](#)

91%
Cyber Attacks
Begin with a phishing email to an unexpected victim

[Deloitte](#)

2,207
U.S. hospitals, schools and governments were directly impacted by **ransomware** in 2023

[EMSISOFT MALWARE LAB](#)

$2.6m
Average cost of a ransomware attack on the U.S. government.

$4.2m
Average cost of a data breach at U.S. Educational institutions
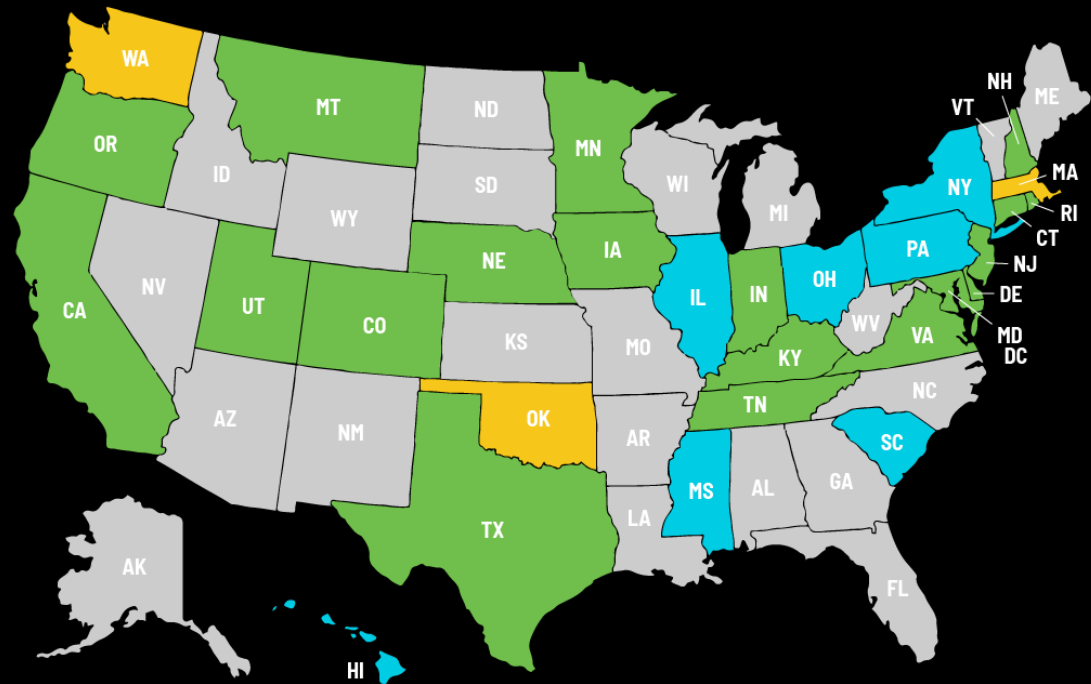
[Ponemon Institute](#)

AI Is making attacks **harder to detect** and **easier to deploy** making them even **more dangerous**.
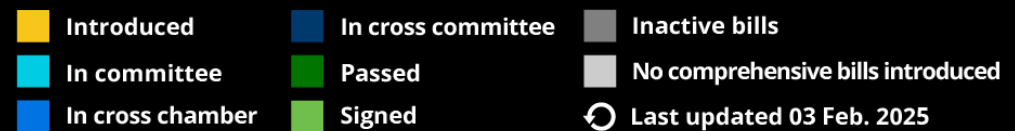
State Privacy Law Map

Utah

H.B. 538 Protection of State Official or Employee Personal Information

Bill Text	Status	Hearings/Debate

Enrolled

Printer Friendly

H.B. 538

PROTECTION OF STATE OFFICIAL OR EMPLOYEE PERSONAL INFORMATION

2024 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kera Birkeland

Senate Sponsor: Michael S. Kennedy

Bill Sponsor:
Rep. Birkeland, Kera

Floor Sponsor:
Sen. Kennedy, Michael S.

Substitute Sponsor: Rep. Birkeland, Kera

Drafting Attorney: Patricia Owen

Fiscal Analyst: Heidi Jo Tak

UTAH | Utah Cyber Center
An official website

UtahID Sign In

Home   Report a Breach   Domain Requests   Gov. Official PII Removal   Resources   ISAC   Cybersecurity Tips   Knowledge Base   Contact Us

Removal of State Elected Official or Cabinet/Senior Staff Personal Identifying Information

State Elected/Cabinet Officials

In accordance with Utah Code §63A-16-109 State elected officials and cabinet level officials or senior staff of the Governor whose life or safety has been threatened in the course of performing the individual's state duties may submit for removal of their personal identifying information from the open web.
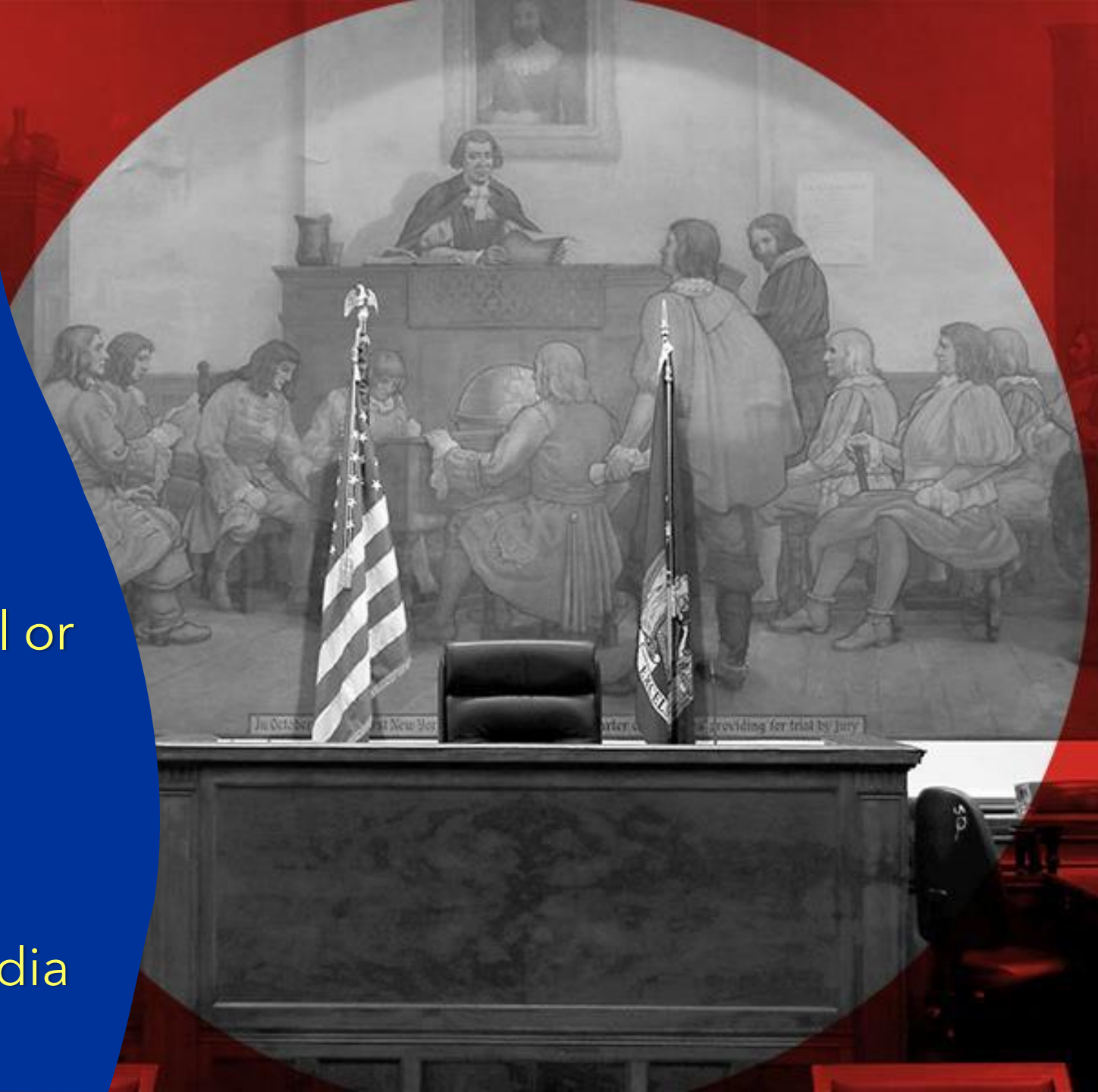
Threat Evolution

* **Motivations Behind Threats:**
    * Ideological disagreements
    * Personal grievances
    * Opportunistic crime (financial or identity theft).
* **Common Starting Points:**
    * Public statements or rulings.
    * Perceived bias or influence.
    * Media coverage or social media posts.

Research Conducted by Attackers

- **Sources of Information:**
  - Public records (property deeds, voter registration, court filings).
  - Social media and public online profiles.
  - News articles and interviews.
  - Leaked databases and breaches.
- **Tools and Methods:**
  - Google searches and advanced search operators.
  - Social engineering and phishing attacks.
  - Data aggregation tools and dark web marketplaces.

History of Attacks on Public Officials

- **Overview of Trends:**
  - Increase in threats correlating with political polarization and online activity.
  - Shift from physical stalking to cyber threats and harassment.
- **Notable Historical Examples:**
  - **U.S. District Judge Esther Salas (2020):** Attack following personal information exposure online.
  - **Gabrielle Giffords (2011):** Assassination attempt tied to public and political profile.
  - **Federal Judges and U.S. Marshals Service (2021):** Documented increase in threats over the past decade.

Item	%
Method of Communicating Threat	
Telephone	31
Multiple	18
Social media	17
Handwritten/Typed	17
Other or Missing	17
Ideological Motivation	
Not Ideologically Motivated	55
Ideologically Motivated	45
Type of Public Official	
Law Enforcement & Military	42
Election/Elected	42
Education	14
Healthcare	9
Specificity of Threat	
Specific Individual	47
Generic Target	30

Threat Surface Reduction

❖ Minimizing Vulnerabilities

❖ Managing communication pathways

Questions