# HOW OUR PERSONAL INFORMATION ONLINE IS USED AGAINST US

Most of us already know companies collect vast amounts of personal data from the websites and apps we visit.

There is clear bipartisan support for more regulation to protect personal information, with 78% of Democrats and 68% of Republicans in favor of government regulation of what companies can do with customers' personal information (Pew Research).

Without meaningful regulation, our personal data is being weaponized by private companies in a variety of ways.

**Insurance Rates –** When you shop online or search health-related topics, companies are collecting this data to create a detailed profile of your behavior. This information can predict your future actions, influence your purchasing decisions, and even determine your risk profile for insurance purposes.

For example, if you frequently search health-related topics, your health insurance rates may increase. If you use fitness trackers, your data may be sold to third-party companies that use it to assess your risk profile or offer targeted advertising.

**Employment and Housing –** Your personal data can also be used to discriminate against you in the job market or when applying for housing. Algorithmic tenant screening tools, which use analytics and artificial intelligence to evaluate rental applicants, perpetuate biases and lead to discriminatory outcomes against low-income individuals and minorities.

Employers are also increasingly using online information to make hiring decisions, leveraging data from social media, professional networking platforms, and other online activities to assess candidates. This can lead to unfair judgments based on incomplete or inaccurate information.

**Identity Theft –** The dragnet of personal information enables bad actors who use it to steal from people, with devastating results.

Companies like NEC Global, Cognitec, and Face++ provide facial recognition technologies used in security, surveillance, and marketing, while biometric data brokers aggregate and sell this information without clear user consent.

When these companies are hacked or leak data, this deeply personal information is at risk of being trafficked by hackers, spammers, and scammers who profit off our identities.