The Always-On Privacy Protection Act

Providing privacy and transparency to
smart device consumers

Privacy

Always-on devices are continuously collecting audio, video, and image data from users.

Transparency

Consumers are unaware of what data is collected and cannot delete the collected data.

Risks

Always-on devices continuously collect data from users, and that data can be commoditized without users' affirmative consent.

In 2015, Samsung Smart TVs' privacy policy allowed for the continuous collection of spoken words and other sensitive information.

Existing Law

1. No regulation of data collection by corporations, advertisers, or the government.
2. No rules governing data retention and sharing for service providers.
3. No prescribed security standards.

Privacy Issues In the News

In 2017, Vizio paid $2.2 million to settle charges that it installed software on its TVs to collect viewing data on 11 million consumers without the consumers' knowledge or consent.

In 2016, law enforcement in Bentonville, Arkansas, sought to obtain data from a murder suspect's Amazon Echo, hoping that the device would contain evidence of the crime.

Legislative Solution

1. Prohibits Always-on service providers from sharing consumer data with third parties without affirmative consumer consent.

2. Provides consumers the opportunity to see and delete any individual data collected and stored by Always-on service providers.

3. Requires law enforcement to obtain a probable cause warrant before accessing Always-on data in a criminal investigation.

4. Requires Always-On service providers to adhere to information security standards set by industry leaders and the FTC.