ASIAN AMERICANS ADVANCING JUSTICE AAJC

A 2026 GUIDE TO BUILDING YOUR

DIGITAL DEFENSE TOOLKIT

01 USE PHONE CALLS, TEXTS, AND EMAIL SERVICES WISELY

To prevent law enforcement from accessing your call and text history, use apps like Signal or Hushed that are not connected to your personal phone number and feature **End-to-End Encryption (E2EE).**

You can enable E2EE on KaKao Talk and Telegram by turning on **"Secret Chats."**

Make a **secondary email account** that is not linked to your personal email address when sending sensitive documents.

Some email providers may share your data with advertisers or law enforcement. Beware of language like:

"We may share data with partners" or
"We scan emails to improve our services"

02 ADOPT SOCIAL MEDIA BEST PRACTICES

Make your accounts private to limit who can see posts, friends, and location. Disable automatic location tracking and **avoid sharing personal information like birthdays or location of work.**

Recent developments in DHS policies allow immigration enforcement officers to review your social media activity from up to 5 years ago.

03 LIMIT ONLINE TRACKING AND TARGETED ADVERTISING

Are you getting ads from DHS about self-deportation? Seeing prices for products that are higher than the prices that others see? *You're getting targeted.*

Opt-out of personalized ads on social media, disable mobile ad ID on your phone, remove location permissions for your apps, and always click "reject all cookies." **Always turn off location services when visiting health clinics, legal offices, or protests.**

04 PRACTICE DIGITAL SECURITY WHEN TRAVELING OR PARTICIPATING IN SENSITIVE ACTIVITIES

If you need to use navigation to reach your destination, use offline apps that work without internet connection.

Be aware that **automatic license plate readers (ALPR's) can track your car's movements across state lines**; consider public transportation or taxis instead.

Turn off Face ID and fingerprint scanning—if your phone is seized, law enforcement can use these to unlock your phone, but not your pin code.

Privacy protections are generally subject to the discretion of border patrol agents at the border.

Consider the political climate and current news cycle when assessing personal travel risk.

05 USE AI CHATBOTS PRUDENTLY AND SPARINGLY

Never put personal information, such as your name, address, case details, immigration status, or identifying information, into AI chatbots.

Chat history is stored and can be used to train future models.

Instead of: "I'm undocumented and need to know my rights if ICE comes to my door."

Ask ChatGPT: "What are the general rights of immigrants during an ICE encounter?"

06 USE SURVEILLANCE CAMERAS AND SMART HOME DEVICES WITH CAUTION

Smart home devices could allow unauthorized users and law enforcement to access sensitive footage, recordings, or device controls *without your knowledge.*

Regularly check device permissions to see who has access to your cameras and smart speakers, or consider removing smart home devices altogether.

07 CONSIDER PRIVACY IN PUBLIC SPACES

Surveillance is highly prevalent in public areas like government buildings, transit stations, shopping districts, and border zones. Be aware that **surveillance cameras, license plate readers, facial recognition technology, and even nearby wireless networks** can be used by law enforcement to identify you.

ICE is using facial recognition apps to speed up their immigration arrests.

Be aware that **these tools are less accurate on Asian faces,** which would lead to wrongful arrests.

If you are in a high-risk situation consider wearing a face mask and hat, turning off Bluetooth and WiFi when you are not actively using them, and avoiding other people who may be taking photos to post online.