Tech Talks: Data Privacy (Android)

Know the settings and apps for increasing your privacy

Android Settings (All Disable/Enable decisions are optional)

Settings	Definitions
Connections > More connection settings > Nearby device scanning *Pixel* *Connected devices > Connection preferences > Nearby Share > Use Nearby Share*	**Nearby device scanning** is a feature used to easily set up connections to other available devices. This feature sends you a notification when there are devices available to connect.
Privacy • Permissions Manager > Call logs, Camera, Location, Microphone, etc. • Android personalization service • Android system intelligence > Clear data • Ads > Delete advertising ID • Usage & diagnostics	**Android personalization service** gives you personalized content based on your app usage (eg text you have entered in one app may appear as a search suggestion in another app) **Android System Intelligence** uses system permissions to provide smart predictions (eg with permission to check your contacts, it will show you suggestions to call a frequent contact.
Location > Location services • Wi-Fi scanning • Bluetooth scanning	**Wi-Fi scanning** looks for Wi-Fi networks and can gather location data and assemble a general idea of your comings and goings. **Bluetooth scanning** searches local area for Bluetooth-enabled devices and requests information about each one.
Google > Manage your Google Account > Data & Privacy • Web & App Activity • Location History • YouTube History • Ad personalization • Personal results in Search	**Ad personalization** does not include content collected from Drive, Gmail and Photos is never used for any ads purposes.
Apps > Three dot menu > Special access > Usage data access *Pixel* *Apps > Special app access > Usage access*	**Usage access** allows an app to track what other apps you're using and how often, as well as your carrier, language settings, and other details. Stock apps should be left alone to ensure proper functionality, but most third-party apps can safely be disabled here.

SANTA CRUZ PUBLIC LIBRARIES

updated 06/15/2022

Tech Talks: Data Privacy (Android)

Know the settings and apps for increasing your privacy

Chrome (open app) > Three dot menu > Settings ● Sync > Sign out and turn off sync ● Search engine > DuckDuckGo ● Privacy and security ○ Clear browsing data > Clear data ○ Always use secure connections ○ Do Not Track	**Sync** can be useful when you want your Chrome passwords, bookmarks, history, etc. across different devices using Chrome. **DuckDuckGo** is a privacy focussed search engine that does not retain search history and use a behavior advertising strategy.
Google Assistant > Google App > Account icon (top right) > Settings > Google Assistant > General > Google Assistant	**Google Assistant** is a convenient feature for using your device hands-free. If your Web & App Activity is disabled then your interactions with Google Assistant are not saved and your audio recordings are not saved.

Privacy Apps (Search, Share, Store)

Type	Example	Benefit
Virtual Private Network (VPN)	CyberGhost	Encrypt your data and mask your location for anonymous browsing
Browser	Brave	Blocks ads, pop ups, and trackers
Messaging/Calling	Signal	Private conversations using encrypted direct messaging
Email	ProtonMail	Private and secure communications with encrypted email service
Storage/Sharing	Tresorit	Files encrypted in transit and rest - Standard storage services reserve the right to access/scan files for illegal content

Resources

- Privacy Planner - https://securityplanner.consumerreports.org
- Virtual Privacy Lab - https://www.sjpl.org/privacy
- Electronic Frontier Foundation - https://act.eff.org

SANTA CRUZ PUBLIC LIBRARIES

updated 06/15/2022

Tech Talks: Data Privacy (Android)

Know the settings and apps for increasing your privacy

More Definitions

- **Advertising Identification** - Unique identifier used to build personal ad profile
- **Behavioral Advertising** - Ads served based on data collected over time
- **California Consumer Privacy Act (CCPA)** - Provide CA residents with following abilities:
    - Know what personal data is being collected about them
    - Know whether their personal data is sold or disclosed and to whom
    - Say no to the sale of personal data
    - Access their personal data
    - Request a business to delete any personal information collected from them
    - Not be discriminated against for exercising their privacy rights
- **Contextual Advertising** - Ads served based on keywords used
- **Cookies** - Data packets exchanged between servers and browsers to identify users and track activity
- **Data Mining** - Finding patterns and connections in data to create new information
- **DNS (Domain Name Server)** - Phone book of the Internet, translates human readable domain names to computer readable IP addresses
- **End-to-End Encryption (E2EE)** - Data encrypted in a way that allows only the unique recipient of a message to decrypt it
- **Internet Browser** - Software application used to access information on the Internet
- **IP (Internet Protocol) Address** - Identifying number assigned to each device
- **ISP (Internet Service Provider)** - Business providing access and use of the Internet
- **Metadata** - data about data
- **TOR (The Onion Router)** - Data encapsulated in layers of encryption and routed randomly through a network of servers to ensure anonymity
- **VPN (Virtual Private Network)** - Service that encrypts your data and masks your location for anonymous browsing