Online Privacy

Online Ecosystem (Stallings, 2019)

- **Online privacy** refers to privacy concerns related to user interaction with Internet services through web servers and mobile apps.
- Websites collect personal information explicitly through a variety of means, including registration pages, user surveys, and online contests, application forms, and order forms
- It also collects personal information through means that are not obvious to consumers, such as cookies and other tracking technologies. *Figure 1* illustrates the many players involved in the online collection and use of personal data.

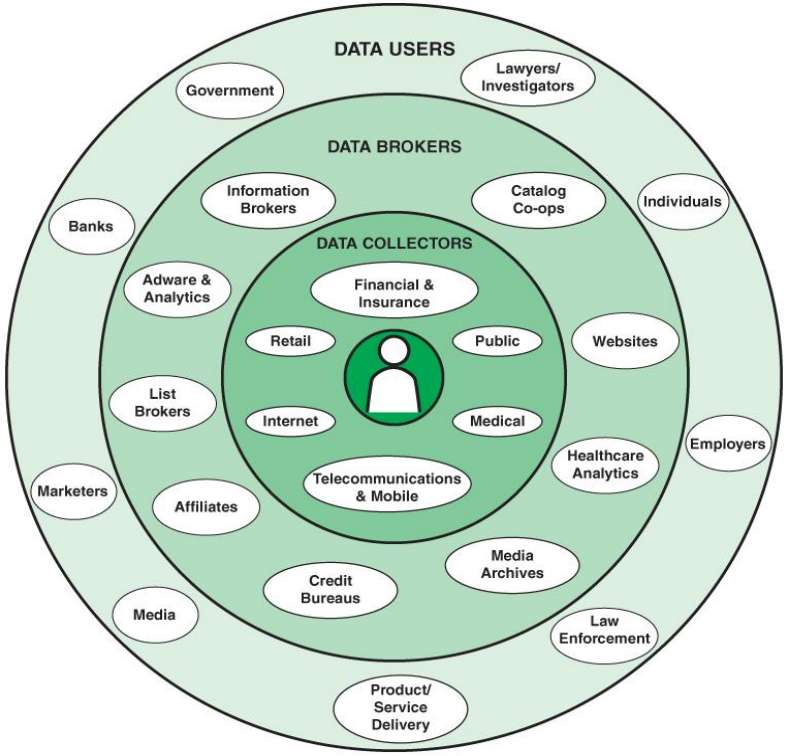

Figure 1. Personal Data Ecosystem

- **Data collectors** collect information directly from their customers, audience, or other types of users of their services.
- **Data brokers** compile large amounts of personal data from several data collectors and other data brokers without having direct online contact with the individuals whose information is in the collected data. Data brokers repackage and sell the collected information to various data users, typically without the permission or input of the individuals involved. Because consumers generally do not directly interact with data brokers, they have no means of knowing the extent and nature of the information that data brokers collect about them and share with others for their financial gain. Data brokers can collect information about consumers from various public and nonpublic sources, including courthouse records, website cookies, and loyalty card programs. Typically, brokers create profiles of individuals for marketing purposes and sell them to data users.
- The **data users** category encompasses a broad range. One type of data user is a business that wants to target its advertisements and special offers. Other uses are fraud prevention and credit risk assessment.

Web Security and Privacy (Stallings, 2019)

- The WWW is fundamentally a client/server application running over the Internet. The use of the Web presents several security challenges:
  - The Web is vulnerable to attacks on web servers over the Internet.
  - Casual and untrained (in security matters) users are common clients for web-based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.
  - A web server can be exploited as a launching pad into a corporation's or an agency's entire computer complex. Once a web server is subverted, an attacker may be able to gain access to data and systems not part of the Web itself but connected to the server at the local site.
- A useful way of breaking down the issues involved is to consider the following classification of security and privacy issues:

- **Web server security and privacy** are concerned with the vulnerabilities and threats associated with the platform that hosts a website, including the operating system (OS), file and database systems, and network traffic.
- **Web application security and privacy** are concerned with web software, including any applications accessible via the Web.
- **Web browser security and privacy** are concerned with the browser used from a client system to access a web server.

Mobile Ecosystem

- The execution of mobile applications on a mobile device may involve communication across several networks and interaction with some systems owned and operated by a variety of parties.

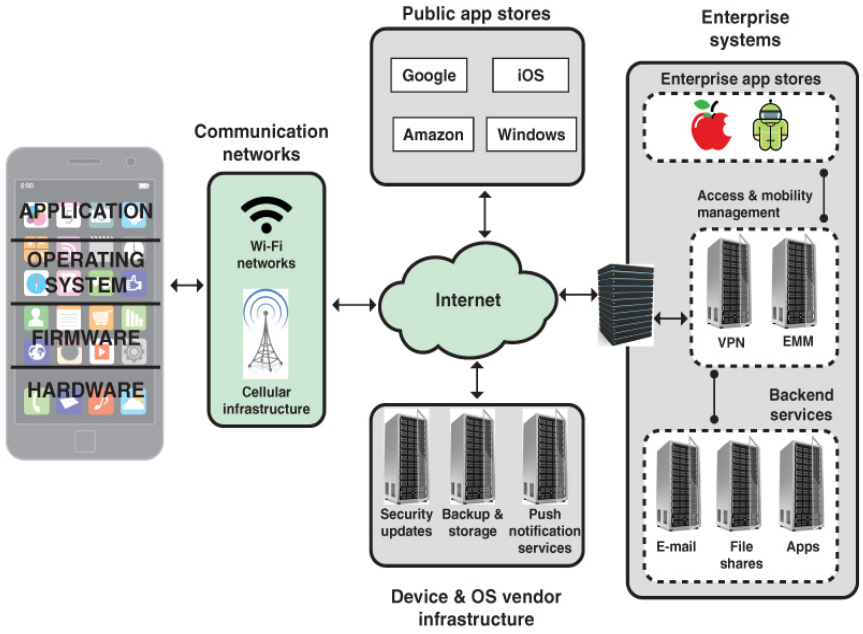

Figure 2. Mobile Ecosystem

- *Figure 2* shows the following elements in the ecosystem within which mobile device applications function:
  - **Cellular and Wi-Fi infrastructure**: Modern mobile devices are typically equipped with the capability to use cellular and Wi-Fi networks to access the Internet and to place telephone calls. Cellular network cores also rely upon authentication servers to use and store customer authentication information.
  - **Public application stores (public app stores):** Public app stores include native app stores; these are digital distribution services operated and developed by mobile OS vendors. For Android, the official app store is Google Play, and for iOS, it is simply called the App Store. These stores invest considerable effort in detecting and thwarting malware and ensuring that the apps do not cause unwanted behavior on mobile devices. In addition, there are numerous third-party app stores. The danger with third-party stores is uncertainty about what level of trust the user or the enterprise should have that the apps are free of malware.
  - **Device and OS vendor infrastructure:** Mobile device and OS vendors host servers to provide updates and patches to the OS and apps. Other cloud-based services may be offered, such as storing user data and wiping a missing device.
  - **Enterprise mobility management systems**: Enterprise mobility management (EMM) is a general term that refers to everything involved in managing mobile devices and related components (e.g., wireless networks). EMM is much broader than just information security; it includes mobile application management, inventory management, and cost management. Although EMM is not directly classified as a security technology, it can help in deploying policies to an enterprise's device pool and monitoring a device's state.

Mobile Application Vetting

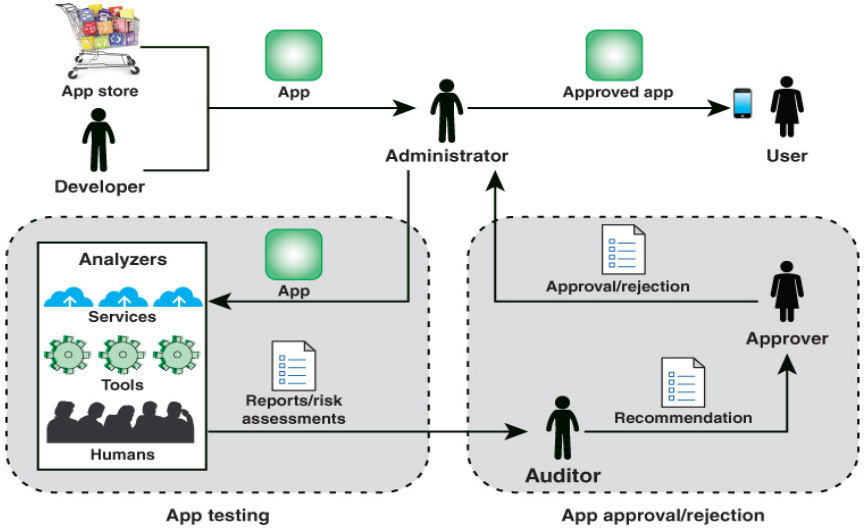

Figure 3. App Vetting Process

- The process of evaluation and approval or rejection of apps within an organization, referred to as app vetting, is illustrated in *Figure 3*. The vetting process begins when an app is acquired from a public or enterprise store or submitted by an in-house or third-party developer.
- An **administrator** is a member of the organization who is responsible for deploying, maintaining, and securing the organization's mobile devices as well as ensuring that deployed devices and their installed apps conform to the organization's security requirements.
- The administrator submits the app to an **app testing facility** in the organization that employs automated and/or human analyzers to evaluate the security characteristics of an app, including searching for malware, identifying vulnerabilities, and assessing risks. The resulting security report and risk assessment are conveyed to an auditor or auditors.
- The role of an **auditor** is to inspect reports and risk assessments from one or more analyzers to ensure that an app meets the security requirements of the organization. The auditor also evaluates additional criteria to determine if the app violates any organization-specific security requirements that could not be ascertained by the analyzers
- The auditor then makes a recommendation to someone in the organization who has the authority to approve or reject an app for deployment on mobile devices. If the approver approves an app, the administrator can then deploy the app on the organization's mobile devices.

Threats from Application

- The first step in developing privacy by design and privacy engineering solutions for online privacy is to define the threats to online privacy. These threats are divided into two (2) areas: web application privacy and mobile app privacy.
- **Web application privacy:** The Open Web Application Security Project (OWASP) top 10 privacy risks project provides a list of the top privacy risks in web applications. The goal of the project is to identify the most important technical and organizational privacy risks for web applications from the perspectives of both the user (data subject) and the provider (data owner). The risks are:
    - **Web application vulnerabilities:** Failing to suitable design and implement an application, detect a problem, or promptly apply a fix (patch), which is likely to result in a privacy breach. Vulnerability is a key problem in any system that guards or operates on sensitive user data.
    - **User-side data leakage:** Failing to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. Leakage may be introduced due to either intentional malicious breach or mistake (e.g., caused by insufficient access management controls, insecure storage, duplication of data, or a lack of awareness).
    - **Insufficient data breach response:** Not informing the affected persons (data subjects) about a possible breach or data leak, resulting in either from intentional or unintentional events; failure to remedy the situation by fixing the cause; not attempting to limit the leaks.

- **Insufficient deletion of personal data:** Failing to delete personal data effectively and/or in a timely fashion after the termination of the specified purpose or upon request.
- **Non-transparent policies, terms, and conditions:** Not providing sufficient information describing how data are processed, such as their collection, storage, and processing. Failure to make this information easily accessible and understandable for non-lawyers.
- **Collection of data not required for the primary purpose:** Collecting descriptive, demographic, or any other user-related data that are not needed for the system. Applies also to data for which the user did not provide consent.
- **Sharing of data with a third party:** Providing user data to a third party without obtaining the user's consent. Sharing results either due to transfer or exchanging for monetary compensation or otherwise due to inappropriate use of third-party resources included in websites, such as widgets (e.g., maps, social networking buttons), analytics, or web bugs.
- **Outdated personal data:** Using outdated, incorrect, or bogus user data and failing to update or correct the data.
- **Missing or insufficient session expiration:** Failing to effectively enforce session termination. May result in the collection of additional user data without the user's consent or awareness.
- **Insecure data transfer:** Failing to provide data transfers over encrypted and secured channels, excluding the possibility of data leakage. Failing to enforce mechanisms that limit the leaking surface (e.g., allowing to infer any user data out of the mechanics of web application operation).

- **Mobile app privacy:** Legitimate mobile apps may be vulnerable to several privacy and security threats, typically due to poor coding practices used in app development or underlying vulnerabilities in the mobile device operating system. Consider the following threats against vulnerable applications, encompassing both privacy and security threats:
  - **Insecure network communications:** Network traffic needs to be securely encrypted to prevent an adversary from eavesdropping. Apps need to properly authenticate the remote server when connecting to prevent man-in-the-middle attacks and connection to malicious servers.
  - **Web browser vulnerabilities:** Adversaries can exploit vulnerabilities in mobile device web browser applications as an entry point to gain access to a mobile device.
  - **Vulnerabilities in third-party libraries:** Third-party software libraries are reusable components that may be distributed freely or offered for a fee to other software vendors. Software development by component or modules may be more efficient, and third-party libraries are routinely used across the industry. However, a flawed library can introduce vulnerabilities in any app that includes or makes use of that library. Depending on the pervasiveness of the library, its use can potentially affect thousands of apps and millions of users.

References:

Kumar, G., Saini, DK., Huy Cuong, NH. (2020). *Cyber defense mechanisms: Security, privacy, and challenges.* CRC Press.
Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technologies, and regulations.* Assison-Wesley Professional. Torra, V. (2018). *Data privacy: Foundations, new developments, and the big data challenge.* Springer International Publishing.