BDA 630:

Legal & Ethical Issues Affecting Big Data

COMPARATIVE ANALYSIS OF PRIVACY POLICIES:

APPLE META GOOGLE

AAKANKSHA SINGH SRIKAR NADIMPALLI BHANU CHANDRA

01

INTRODUCTION

The privacy policies of Apple, Facebook, and Google are not only long and complicated but also crafted to reflect each company's business model. Apple earns most of its revenue through device sales and subscriptions, so it consciously chooses to position itself as being privacy-focused. Facebook (Meta), on the other hand, builds its business around advertising driven by detailed user profiling. Google straddles both worlds—offering services like Gmail and Android while maintaining a massive advertising ecosystem. In this presentation, we explore how these business models shape their data practices: what kinds of data are collected, how it's obtained, how much control users really have, and how these practices hold up under laws like the GDPR and CCPA.

02

What Kind of Data Is Collected?

APPLE

Apple's privacy policy emphasizes that it tries to collect "only the personal data that is necessary." The company gathers device-related identifiers (like your Apple ID, serial number, and IP address), usage data (such as app usage and crash logs), and user-provided information (name, email, payment info). Optional data—like Siri interactions, Health data, and photos—is collected only if the user enables those features. Apple also stores analytics data, but claims it is anonymized through techniques like differential privacy.

META

Facebook collects nearly everything a user does on and off its platforms. This includes user-generated content (posts, messages, comments), profile information, photos, biometric data (facial recognition where enabled), and activity data across the internet via the Facebook Pixel. It tracks IP addresses, device characteristics, browser fingerprints, and even mouse movements. Metadata like when and where messages were sent, the people you interact with most, and interactions with ads are also collected. Third-party data brokers and partners also supply user-related data to Facebook.

GOOGLE

Google collects information from virtually all of its services: search history, emails, voice commands to Google Assistant, calendar events, location data, app activity, browsing history (especially through Chrome), and interactions on YouTube. Google's account-level data consolidation means that activity across all Google services is tied to a single user profile. Google also receives vast amounts of data through third-party apps and sites using services like Google Analytics, AdSense, and embedded services like reCAPTCHA.

03

How Is the Data Collected?

APPLE

Apple collects data primarily through direct user interactions and device sensors. iPhones, for example, track location data via GPS and Wi-Fi, but users can control this in settings. Analytics data is gathered automatically unless turned off. Siri voice requests are sent to Apple's servers for processing only when Siri is actively triggered. iCloud uploads documents, contacts, and backups, which Apple encrypts in transit and at rest—though in many cases, Apple holds the encryption keys.

META

Facebook collects data both actively and passively. Active data includes everything users post, upload, or interact with. Passive collection happens through cookies, tracking pixels, social plug-ins (like buttons), and logins using Facebook credentials. Facebook tracks users even when they're logged out or on non-Facebook sites, which is possible due to cookies and browser fingerprinting. Partner companies share purchase data and offline behavior via APIs like Facebook Business Tools.

GOOGLE

Data collection is baked into all Google services and products. For example, Google Assistant constantly listens for the "Hey Google" wake word, and Chrome syncs browsing and search history with your Google account unless explicitly turned off. Android devices send telemetry data back to Google regularly. Through APIs like Firebase and tools like Google Tag Manager, Google tracks user activity in countless mobile apps and websites—even those not run by Google.

04

What Kind of Choice Do Users Have?

APPLE

Apple allows users to opt out of data collection features like targeted ads, location services, and Siri recording storage. iOS includes a system-wide “App Tracking Transparency” setting, requiring apps to ask for permission before tracking across other apps or websites. Users can also disable iCloud or choose local-only storage for health or photo data. However, some device analytics and usage data collection cannot be fully disabled.

META

Facebook presents its privacy choices in a complex network of menus, often under “Settings & Privacy.” Users can choose ad preferences, manage who sees their data, and turn off facial recognition. However, Facebook reserves the right to collect and use data under “legitimate interests,” including data gathered from third-party sites and apps. Opting out of personalized ads does not stop data collection—it only stops the personalization of ads.

GOOGLE

Google’s “My Account” dashboard offers controls to pause search history, YouTube watch history, and location tracking. Users can review and delete stored data through the “My Activity” page. However, some data (such as system logs or telemetry) continues to be collected for “service functionality” or “security” reasons, and opting out of data collection often reduces service quality or disables features.

05

With Whom Is the Data Shared?

APPLE

Apple shares data with service providers (such as payment processors and cloud infrastructure vendors), but claims these providers must follow Apple’s privacy terms. Apple says it never sells personal data and limits third-party tracking. It does not allow third-party ad tracking in native apps without explicit user permission.

META

Facebook shares data within the Meta family (including Instagram, Messenger, and WhatsApp) and with third-party advertisers, app developers, researchers, and external vendors. It uses terms like “trusted partners” or “vendors” without clearly defining them. Facebook’s “Off-Facebook Activity” tool reveals how extensively it tracks and shares user data across the web.

GOOGLE

Google shares data across its internal services (e.g., Gmail and YouTube) and with third parties such as advertisers, publishers, developers, and analytics providers. Google insists it does not “sell” personal information—but its advertising platforms (like Google Ads and AdMob) rely on user data for profiling and targeting. Data is shared in anonymized or aggregated form, but this may still be sufficient for re-identification.

06

Language and Framing in the Policies

APPLE

Apple’s privacy language is clear and user-centric, frequently using definitive statements like “we do not sell your personal information.” But even Apple includes conditional clauses such as “unless required by law,” allowing data to be shared with governments or law enforcement.

META

Facebook’s policy is full of permissive, open-ended language: phrases like “we may collect,” “we typically use,” or “we could share with affiliates” give Facebook wide leeway. The use of “trusted partners” or “legitimate business purposes” is particularly vague.

GOOGLE

Google’s policy uses similarly flexible language. It frames data collection as being “to make our services better” and often relies on phrases like “we may use information for purposes such as...” without committing to exact uses or limits. These choices in language are strategic—they reduce liability while allowing for maximum data exploitation.

07

Compliance with GDPR

APPLE

Generally aligns with GDPR standards. Users can request access to their data, correct it, or delete it. Apple uses consent as the primary basis for most sensitive data collection and provides transparency reports about data requests from governments.

META

Has faced multiple GDPR violations. In 2023, Meta was fined over €1.2 billion for failing to comply with GDPR data transfer rules. The company's use of broad "legitimate interests" to justify tracking and the complexity of its consent flows have been legally contested multiple times.

GOOGLE

Google has also been penalized—most notably a €50 million fine in 2019 for not properly informing users about data collection in Android setup flows. While Google has added more robust user controls, it still faces scrutiny for default settings that nudge users into agreeing to tracking.

08

Compliance with CCPA

APPLE

Google has also been penalized—most notably a €50 million fine in 2019 for not properly informing users about data collection in Android setup flows. While Google has added more robust user controls, it still faces scrutiny for default settings that nudge users into agreeing to tracking.

META

Insists it does not “sell” personal data, but this has been heavily criticized. The California Attorney General warned that personalized advertising may qualify as a sale under CCPA definitions. Facebook provides a “Do Not Sell My Personal Information” page, but it is not prominently displayed, and the company often shifts the burden of enforcement onto the user.

GOOGLE

Similar to Facebook, Google offers a “Do Not Sell My Info” option but disputes the idea that ad targeting constitutes a sale. Still, under CCPA, Google does allow Californians to request data deletion and opt out of ad personalization, though some settings are buried deep in the account menus.

09

WHY/WHY DON'T THEY COMPLY

APPLE

Apple largely complies with both GDPR and CCPA because its business model is less dependent on advertising and extensive user tracking. Apple emphasizes privacy-by-design, offers strong data access and deletion tools, and avoids selling user data. However, certain loopholes, such as mandatory device analytics and the retention of some deleted account markers, show that compliance is not absolute.

META

Facebook (Meta) struggles significantly with compliance. Although Facebook provides users with access and deletion options, its reliance on broad "legitimate interests," opaque sharing with "trusted partners," and complex opt-out processes have led to multiple GDPR violations and fines. Under CCPA, its definition of "selling" data remains contested, and opt-out mechanisms are often difficult to navigate, suggesting incomplete compliance.

GOOGLE

Google offers extensive user controls and has improved transparency, positioning itself closer to compliance. Yet, Google's expansive data collection across services, default-on tracking, and debates around whether ad targeting constitutes a "sale" under CCPA expose compliance gaps. Regulatory actions, including fines, indicate that despite strong legal frameworks, full adherence remains aspirational.

Summary and Key Differences

Apple stands out for collecting relatively little data and offering clear controls. Its privacy stance is aligned with its business model and includes strong protections, though not total immunity from tracking.

Facebook collects a vast amount of data and shares it widely under unclear terms. Its complex settings and vague language frequently undermine user control.

Google’s data collection is expansive and well-integrated across services, with more transparent controls than Facebook but similar reliance on default-on tracking.

BDA 630:

Legal & Ethical Issues Affecting Big Data

THANK YOU

APPLE META GOOGLE

AAKANKSHA SINGH SRIKAR NADIMPALLI BHANU CHANDRA