Project 6:
Digital Privacy Agreement Audit
A Data Ethics Project

Group 7

Richard Hoehn (**richardhoehn**)

Hector Rogel (**rogel9007)**

Isaiah Osborne(**IMOsbo**)

Karson Woods (**Kwoods132**)

Overview of Services Analyzed

In relation to the Service of Travel, the matrix reveals that CBP-Govt. plays a central role in security-driven data collection and processing, including facial recognition for identity verification, primarily for non-citizens. Unlike the commercial entities, CBP does not offer standard consumer opt-out rights or rely on consent mechanisms—its processing is narrowly focused on lawful, national security purposes. In contrast, Viasat, which may be relevant in the travel service context for connectivity, supports consumer rights and data minimization in line with CCPA, VCDPA, and GDPR standards, providing greater transparency and opt-out capabilities.

Across the financial services analyzed, they had very similar privacy statements. They all collected browsing information, such as search data, cookies, and geolocation. Any communication activities on their different programs were recorded and kept Overall, these privacy . However, Capital One expressly collected information for the purposes of marketing other products, while PNC Bank only collected that information for their personal use. Interestingly, despite collecting more data, Capital One actually had a more robust opt-out system, allowing you to opt out of data collection by setting the Global Privacy Control in your browser, while PNC Bank actually required a phone call to opt out of marketing sharing. Despite this, the two privacy policies were roughly the same in terms of detail and coverage.

Across the music services, Spotify and YouTube Music, there was much more variation in the quality of the privacy policies. Spotify, an European company, has an extremely robust list of all the data collected, with strong explanations for why they collect the data. While Spotify still collects just as much data as other services, they do seem much more up front about what data they collect and why.

Additional analysis was also focused on Gmail, Cash App, Discord, and Netflix. These are services spanning from communication, finance, and entertainment. These platforms vary significantly in data collection and user right transparency. Gmail, operated by Google, provides the most comprehensive data controls through tools like Google Takeout. In contrast, Cash App collects sensitive financial data with limited portability options. Discord stands out for its minimal advertising model and strong control over message history while Netflix offers basic data access but limited opt-out options. These examples demonstrate the spectrum of privacy protections in consumer-facing services.

We also analyzed Pearson, Etsy, Instagram, and Udemy which spanned educational tools, e-commerce, and social media. Their privacy policies varied heavily with the two educational tools' (Pearson and Udemy) privacy policies not sharing many similarities surprisingly. Etsy handles a surprising amount of sensitive information including biometric data as part of their data collection processes. Instagram in comparison to these other ones don't collect as much sensitive information from what I was able to gather. Another interesting point of their privacy policies was that Instagram had no opt-out available whereas the other ones did.

Key Findings from Comparison

Finding regarding IKEA's privacy policies appears to be the most open among the entities reviewed. Its privacy policy is written in clear, user-friendly language, offers layered transparency, and provides GDPR-style rights with strong emphasis on user control, consent, and opt-out mechanisms. Compared to Aerton, Viasat, American Airlines, and CBP, IKEA demonstrates a greater commitment to explaining data practices and empowering users through accessible choices and consistent policy updates.

A consistent pattern across the services was the collection of core user names, emails, and device information regardless of the platform's purpose. However, differences emerged in transparency and user empowerment. Gmail offered detailed settings and export options showing high user control. Cash App and Netflix, while compliant with basic U.S. privacy standards, buried critical privacy choices within their apps or failed to notify users directly of policy changes. Discord had fewer opt-outs but benefited from not engaging in targeted advertising. These differences suggest that user control is more dependent on corporate priorities than on regulation alone.

Regulatory Compliance Assessment

IKEA demonstrates the strongest overall regulatory compliance, especially in alignment with GDPR standards. It offers clear and layered privacy notices, emphasizes explicit and informed consent, and provides users with full rights (access, correction, deletion, objection, and withdrawal of consent). Its policies are regularly updated and transparent.

CBP, as a government agency, operates under different legal frameworks and is exempt from most commercial privacy laws like CCPA or GDPR, so its compliance is tailored to DHS regulations, not broader consumer data protections.

Among the communication and entertainment services reviewed, Gmail demonstrated as one of the highest alignment with GDPR and CCPA regulations, offering explicit consent management, comprehensive notice, and full data portability. Cash App and Netflix met baseline CCPA standards, such as providing access and deletion rights, but lacked robust opt-out systems and often implied consent through use. Discord complied with key principles like access and deletion, but lacked clarity around data export and consent mechanisms. Overall, while all four met minimal regulatory thresholds, only Gmail reflected a proactive commitment to user rights and compliance.

While both Spotify and YouTube Music have GDPR related privacy policies, breaking from the US-only privacy policies of Capital One and PNC, Spotify has a much more robust GDPR privacy policy, which is perhaps to be expected. In comparison to the international companies' strict adherence to global privacy laws, neither PNC Bank or Capital One ever had any policies related to GDPR, which makes sense based on their geographic scope.

Both Spotify and Google allow users to delete and export their data under GDPR protection, but interestingly, Spotify adds an additional caveat that your data will not be "subject to automated decision making." While this statement is somewhat vague, leaving its true purpose up to interpretation, Google does not have a similar disclaimer.

Looking at the educational tools we evaluated, Udemy had some interesting differences in privacy policies compared to Pearson. With respect to GDPR, Pearson had separate entities called Pearson Education Limited and Pearson UK Limited to cover the United Kingdom and Europe. In addition to this, Pearson itself still specified certain rights regarding residents of the EU and UK. In contrast, Udemy transfers data from users outside the US to the US and processes it there. They don't specify why this is done, but one can presume this is done to avoid GDPR requirements and avoid offering certain rights and protections to users in the EU and UK.

Recommendations for Improvement

Digital services should adopt a layered privacy notice approach, making essential rights and data uses immediately visible to users. Platforms like Cash App and Netflix should follow Gmail's example by offering centralized privacy dashboards and clear opt-out paths. Discord could improve by enabling greater portability and granular consent choices. Especially around cookies and analytics. Broadly, services should notify users directly of privacy policy updates rather than expecting them to check for changes. Enabling users through transparency and control should become an industry standard. Not just a regulatory requirement.

Additionally, supporting the Global Privacy Control would be a strong improvement, allowing users to easily opt out from data collection across all of their different web browsing and service usage. Some companies already support this; having wider support would make it easier for web users to make privacy-focused decisions. Spotify's additional caveat of ensuring your data remains safe from AI overreach is also an unique proposition and likely to become more prevalent as AI technologies grow. Notably, the main AI company surveyed, Google, has not adopted this standard yet, which is perhaps an interesting referendum on their AI privacy standards.

Lessons Learned

This comparison highlights how companies vary widely in transparency and regulatory compliance. IKEA sets a strong ethical example by embracing GDPR principles—prioritizing user consent, data minimization, and clear communication. In contrast, U.S.-based companies like Viasat and American Airlines align more with CCPA but offer less emphasis on user empowerment. The key lesson: ethical data practices go beyond legal minimums—true privacy protection requires clarity, choice, and accountability.

This project also revealed how deceptive digital privacy policies can be. While most companies technically comply with laws like CCPS or GDPR, they often design interfaces to discourage users from asserting their rights. The presence of "dark patterns", such as hidden or confusing opt-out processes, illustrates how compliance can fall short of ethical practice. Ethical data handling requires intentional design that respects user time, autonomy, and trust. Ultimately, privacy is not just a technical or legal matter. It reflects the extent to which a company genuinely values its users.