Humanize before you submit

Likely Turnitin score: **15-50%** - likely over 20%

Humanize the colored text

Keep humanizing until this report says Ready to submit.

Once the title says Ready to submit, you're covered: if Turnitin flags it after that, get a free month of Pro Bundle ($14.99) - plus $25 if the text came straight from our humanizer. This report isn't covered yet. See terms

Reads as AI - catches 83 of 100 sentences Turnitin flags

Borderline - with blue, catches 95 of 100; marks a bit more than Turnitin

Measured on 1,707 Turnitin reports of 20% or more, October 2026. Papers vary.

Highlights are our estimate - Turnitin may mark other sentences.

EliteWorks is not affiliated with Turnitin.

Given the rapid advances in data processing, privacy law asks which jurisdiction can provide meaningfully actionable legal boundaries instead of stating aspirational principles protecting data processing. The Foundations materials show two patterns from prior materials in the two jurisdictions. In the United States, privacy reflects concerns about individual liberty and choice. In Europe, privacy is conceptualized as a legally enforceable fundamental right. There are real world consequences from this divide that go beyond theory. The widespread use of inferential, predictive, and decision influencing data processing means that models that rely on individual agency will diminish in usefulness. In that respect, the European model provides a more sustainable starting point for privacy protection in the long term. The United States public sector model is an example of how far legal process can deformation of law (or legal process) in place of a real right to privacy framework. The “reasonable expectation of privacy” doctrine is significant because it requires courts to confront the question of whether governmental surveillance is justifiable, and whether such surveillance is an intrusion. The doctrine was designed for single, isolated acts of surveillance. It does not account for the continuous system of surveillance that exists in contemporary governmental data collection, storage, linking, and reuse practices.

Although the Privacy Act of 1974 aims to respond by granting individuals access and correction rights, its practical force is often shaped—and limited—by narrow administrative definitions of what counts as a covered “system of records.” As a result, regulation can drift toward compliance formalities and documentation, while leaving the deeper question—how government data is actually repurposed across contexts—only weakly constrained.

A similar problem exists in the private sector. The U.S. privacy regime is also sectoral, meaning that the legal obligations depend on the industry and the type of organization that is processing the data. This can create a clear set of rules in a given industry, but the data itself does not honor those distinctions. From the user’s point of view, tracking is continuous across apps, devices, and services, and the data flows freely through brokers, ad-tech, and related services. When the same data is subject to different rules merely because it is processed by different people, it is no surprise that there are predictable gaps.

The enforcement mechanism is also geared towards whether the company lied about its behavior, as if privacy is a problem of deception rather than a problem of power and subsequent use. This is based on the notion that “notice and consent” provides a meaningful control for consumers. In reality, most people cannot reasonably read, compare, and negotiate privacy policies, and opting out may mean forgoing access to vital services.

Through institutional constraints, not individual vigilance, we can ensure that organizations have the appropriate protections in place against unauthorized access or misuse of their customers' personal information. Just as every organization should have a means of verifying that only those individuals who are authorized to access customer information, each organization should also have guidelines for determining whether they are using that information for the primary purpose for which it was collected. Likewise, commercial businesses should have guidelines regarding how to extend the use of that information beyond what is required under the law. Such an approach should provide businesses with a means of complying with the requirements of the law while at the same time providing consumers with greater privacy and control over their personal information. In the end, the European model is a more reliable foundation for privacy protection because it places a higher degree of responsibility on the business than does the U.S. model. Although the U.S. model fosters innovation, the predominant emphasis on the individual means that it is less effective in an environment where data is continually being transmitted back and forth. Ultimately, organizations will need to create limits on the extent to which they use personal information before they are able to protect the privacy of their employees’ data.