

Reframing Privacy: Regulators, Firms and the New American Metric

By Kenneth A. Bamberger & Deirdre K. Mulligan

The sufficiency of U.S. information privacy law is the subject of heated debate. A majority of privacy scholars and advocates contend that the existing patchwork of U.S. regulation fails to ensure across-the-board conformity with the standard measure of privacy protection: Fair Information Practice Principles (FIPPS) first articulated in the early 1970s. U.S. law, they argue, further falls far short of the EU's omnibus privacy regime thereby failing to protect against a variety of privacy based harms. A smaller group of scholars similarly fault the U.S. for latching onto a watered-down version of FIPPS that emphasizes the procedural requirements of notice and individual choice to the exclusion of a substantive consideration of the harms and benefits to society as a whole that result from flows of personal information, and in the process created bureaucracy in lieu of privacy protection.

These critiques' positive claims regarding U.S. law's departure from FIPPS are largely true. Yet, we argue, these debates generates far more heat than light as to the question of what laws provide meaningful privacy protection. The emphasis on measuring U.S. privacy protection by the FIPPS metric simply misses the mark, focusing on a largely procedural standard offers limited utility in guiding corporate decisionmaking to protect privacy. It thus ignores important shifts in the conception of privacy—and therefore, perhaps, how the success of its protection should be assessed—in the United States.

This paper—the first in a series drawing on a qualitative empirical study of privacy practices in U.S. corporations—argues instead that FIPPS no longer represents either the exclusive goal of U.S. privacy policy or the sole metric appropriate for assessing privacy protection. By contrast, this article demonstrates that U.S. information privacy policy over the last decade, as understood by both regulators and those firms implementing privacy measures through regulatory compliance, evidences a second—and very “American”—definition of informational privacy. As demonstrated both by the institutional choices regarding privacy regulation and by qualitative data regarding corporate privacy practices, informational privacy protection in the U.S. today is rooted, not in fair notice and process, but in substantive notions of consumer expectations and consumer harm. The corporate practices resulting from the “expectations and harm” definition of privacy, in turn, often offer the promise of far greater substantive privacy protection than any FIPPS regime could provide.

This initial effort to inquire as to how the form and oversight structure of information privacy law influences its implementation and effect illustrates the value of “holistic evaluation(s) of privacy protection systems” recommended by Charles Raab. Looking at rights and obligations on paper is insufficient to guide policy: better privacy protection requires analysis of how law works in the wild.