In a world in which anybody and everybody seems to have an opinion about the meaning of privacy and the extent to which it is eroding and/or transforming in the light of technological developments, it is refreshing to find a deeply considered, and richly documented, book that advances a genuinely different theory about the subject. Given the number and diversity of scholars who have attempted in the past to define what privacy is and is not, it is indeed a brave scholar who would venture to advance an original conceptual and theoretical framework. Helen Nissenbaum has taken on that challenge. And every software developer, CEO, futurist, or technological guru who has seen fit to pronounce on the nature and future of this complex subject should read Privacy in Context carefully.

Many privacy and surveillance scholars will already know of Nissenbaum’s work, as the ideas reflected in this book have been nurtured over a period of time in consultation with academics from different disciplines. Nissenbaum is herself a philosopher, but the book is interdisciplinary and admirably informed by work from different areas of the social sciences and humanities. And in outlining the major trend in the development and impact of ‘socio-technical systems’ she also displays an impressive knowledge of the capacities of contemporary networked technologies. The premise for the work is that the privacy issue is transformed by a technological environment that can keep track of individuals, ‘know us better than we know ourselves’ and which possesses a capacity to ‘spread and find anything, everywhere’. The scope, complexity and depth of these practices have changed institutions, power structures and relationships, and necessitate a rethinking of traditional concepts and approaches to privacy protection and, by inference, to surveillance.

Nissenbaum’s critique of the privacy literature is compelling. Whether framed as a constraint on access to personal information, or as a form of personal control, privacy definitions are wanting. Privacy has both normative and analytical purposes. It is both a core and an instrumental value. The analysis of the protean and confusing conceptual terrain is nothing new. Nissenbaum argues, however, that the confusion has serious consequences for the effective analysis of socio-technical systems, and the ability to make clear moral claims about the distinction between the justifiable and unjustifiable processing of personal information.

More compelling, I think, is Nissenbaum’s critique of the public vs. private dichotomy, which has limited the normative scope of privacy and severely restricted political discourse. Privacy is associated with not one but three dimensions of the public/private distinction, in terms of actors, space and information. These dimensions are often conflated, producing sloppy reasoning and self-serving arguments. Despite a superficial elegance, one cannot restrict privacy rights and claims to the domain of the ‘private’ because
contemporary socio-technical systems have blown away these clear distinctions. Thus, ‘there are no actors, no spheres, no information that can be assigned unconditionally to the domain of the public, free of all and any constraints imposed by rights of privacy; none are “up for grabs”’ (p. 126).

Nissenbaum is less concerned with locating ‘the’ value of privacy than with understanding when and why new systems provoke legitimate concern and resistance. Key to this understanding is a belief that a right to privacy is ‘neither a right to secrecy nor a right to control but a right to appropriate flow of personal information’ (p. 127). The key to these complex questions lies in an understanding of ‘social context’ and ‘context-relative informational norms’. The variability in these norms is not arbitrary but contingent on the types of information, the roles of subject, sender and recipient, and the principles under which the information is transmitted within structured social settings. These settings possess a contextual integrity, which cohere over time. Much of the discomfort and indignation we feel as a ‘privacy invasion’ stems, Nissenbaum contends, from a disruption of that integrity. The theory is closely related to, but deeper than, conceptions of a ‘reasonable expectation of privacy’, the principle that has guided much privacy jurisprudence in the English-speaking world. The right to privacy is, then, ‘a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention, but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones’ (p. 231).

Nissenbaum extends this framework into a more systematic decision-heuristic to determine how new practices vary from the prevailing social context. Does the new practice bring about changes in recipients, subjects and senders? Does it alter the type of information transmitted? Does it entail a revision in the principles governing the transmission? If the answer to any of these questions is in the affirmative, then the practice is flagged as violating entrenched informational norms, constituting a prima facie infringement of contextual integrity, a presumption, which may only be overcome if the new practice can be demonstrated as morally superior. This judgment leads to a necessary discussion of the moral philosophy that would permit departures from accepted practice, as well as to some admittedly sketchy applications in a variety of organizational contexts.

By now my respect for Privacy in Context should be obvious, and any serious critique deserves far more space than is available in this review. Furthermore, it is quite apparent that Nissenbaum is entirely familiar with the range of objections to her argument that have, and might be, advanced and responds respectfully to several along the way. An obvious question is how ‘contexts’ are, or should be, distinguished from one another. The challenge is crucial, and obviously difficult. Some contexts may be more or less institutionalized, granular, stable, and overlapping. Should the sharing of personal information on a work-related injury, for instance, be guided by the norms of the employment context, the health-care context, or the insurance context? Thousands of similar examples could be advanced. For Nissenbaum, these types of problem do not refute the context-based structure of social life, and the need to understand privacy violations in this light.

I am persuaded that contextual integrity does shed important light on why and how people do, and should, respond to privacy violations, and advances the debate beyond the typically crude clashes between privacy and the ‘public interest’. I am less persuaded that it serves as a reliable guide to policy and system design, or to jurisprudence. Does it really add much to the principle that has been at the heart of the theory and practice of information privacy from the outset—that of ‘reasonable purpose’? Most laws, codes and standards are founded on the principle that organizations should only be capturing, managing, storing and sharing personal data that is necessary or relevant for a defined, and transparent, set of organizational purposes. If they wish to use that information for a secondary purpose, they should, under most circumstances, obtain informed consent. Leaving aside the question as to whether these laws are effective, I am left wondering whether Nissenbaum’s theory is actually saying much more than this. There is a great deal in her analysis of context, which emphasizes the purposive elements within social contexts. Thus, ‘purposes are not merely important properties of contexts, they are partly constitutive of them’ (p. 166). Further, when I think through some of the thorny privacy dilemmas offered in the text, Nissenbaum’s
conclusions from a contextual integrity perspective, do not differ substantially from mine generated through a ‘relevance to purpose’ test.

One of the reasons, I think, that she has not engaged with this obvious, and somewhat different, framework is that this tends to emanate from countries other than the United States, which have comprehensive privacy or data protection regimes, applying to all personal information processing regardless of institution, technology or ‘context’. Nissenbaum’s work stands in a long line of important scholarship that has tried to offer guidance for American legislators, regulators and courts. She admits in the Introduction that most of the examples are taken from the US, but also contends that there is no reason why her theory of contextual integrity cannot be more generally applied. I am sceptical, not because the theory is not sufficiently general, but because most other countries, for better or worse, have already gone down a rather different path, and invested considerable resources in a more comprehensive statutory approach to information privacy.

Nissenbaum generally concedes this point when she contends that the American approach ‘may be the more promising one as, at its best, it embodies informational norms relevant to specific sectors, or contexts, in the law’ (p. 238). If that is the case, then I worry that her theory of contextual integrity might be appropriated to prop up a continued patchwork of federal and state laws that leaves many gaps and provides only partial rights and remedies. If anything, the interconnectedness of social-technical systems renders it all the more difficult to carve up the information economy into discrete ‘sectors’ amenable to precise regulation. That said, all privacy regulation needs sensitivity to the informational norms generated by social contexts. A close reading of Privacy in Context will reward any person who knows intuitively that privacy is a crucial social value, but also worries that the policy and legal solutions to date have been inadequate.