Book Review

Solove, Daniel J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
282 pp, Paperback, \$18.95 (US), ISBN-10:0814740375.

Allison Kenner

Rensselaer Polytechnic Institute, New York, USA. <mailto:kennea2@rpi.edu>

Thanks to digital dossiers, we now have less knowledge and control over our public profiles than ever before. Beyond concerns over the vast amounts of personal information collected, and the ever-more efficient exchange between an increasing number of parties, what may be most troublesome about digital dossiers is the discreet erosion of privacy and the absence of mechanisms to halt it. Daniel J. Solove's *The Digital Person: Technology and Privacy in the Information Age* investigates this contemporary dilemma—how information technology has enabled progress while leaving personal rights vulnerable. The book analyzes the kinds of problems that arise from digital dossiers, exploring the importance of information privacy, how it is slipping away, and what needs to be done to salvage personal rights. According to Solove, today's privacy problems stem from a legal framework that is insufficient to address social and technological changes. It isn't the absence, but the inadequacy of outdated privacy laws that make digital dossiers difficult to regulate. Part of the problem, Solove argues, is a poorly conceived definition of privacy. *The Digital Person* addresses this by providing a digestible and innovative road map to information privacy in the United States, describing how digital dossiers are created, how data flows leave personal information vulnerable, the extent to which business and government facilitate the process, why this is troublesome and how regulation can safeguard individual rights. Central to this overview is a reconceptualization of 'privacy,' something that has largely been missing from contemporary discussions.

Historically, privacy law has been most closely associated with innovations in communication and media. Two of the book's most prominent examples concern the U.S. postal service and journalism. While never clearly articulated in the U.S. Constitution, early political leaders such as Thomas Jefferson and Benjamin Franklin did express concern over personal privacy, particularly in regard to the postal service (225). This led to several laws, still in effect today, that protect the contents of mail. Most privacy law leans on the Fourth Amendment, which prevents the government from "unreasonable search and seizure" and provides the foundation for what Solove refers to as the secrecy paradigm. Here, privacy refers to the concealment of an individual's hidden world and is "invaded by watching and by public disclosure of confidential information" (42). This idea can be seen in legislation, such as the Federal Communication Act of 1934 and Electronic Communication Privacy Act of 1986, where personal communication is understood to be private or hidden, and thus beyond the government's reach. A second example stems from late nineteenth century journalism and photography, which gave rise to a new set of privacy threats. This was addressed in *The Right to Privacy* (1890), written by Boston lawyers Samuel Warren and Louis Brandeis, a publication widely considered to be the foundation of privacy law. From this article, courts and legislatures established a number of privacy torts, falling within four distinct categories: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation. Communication laws and privacy torts both use the secrecy paradigm and the notion of invasion as a foundation for personal rights. Yet neither secrecy nor invasion seem to be at issue with digital dossiers. The information contained in computer databases aren't much of a secret. Details such as age, gender, residency, and social security

Kenner, Allison. 2009. Review of Solove's *The Digital Person: Technology and Privacy in the Information Age*. *Surveillance & Society* 6(2): 193-194.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© Allison Kenner. 2009 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

numbers are a standard part of government records, and are often given voluntarily or are accessible through public documents. If invasion of privacy in the traditional sense doesn't characterize the means by which digital dossiers are created and used, how can concerns over the increased collection and exchange of personal information be more accurately defined?

Building on this nuanced discussion of privacy law, Solove draws on literary metaphors to explore cultural and political understandings of privacy. George Orwell's Big Brother is the dominant figure in this discourse, one that highlights the overarching power of government and helps facilitate discussions about control of information. *The Digital Person* dismantles this metaphor, at least as a description for the harms associated with digital dossiers. Attractive and accessible as it may be, Big Brother doesn't really characterize the dynamics of information gathering and sharing; the growth of databases has been less orchestrated and more benign than the government Orwell describes. Big Brother typically calls to mind an all-knowing surveillance system where privacy and individualism are squashed, aims and power relations that do not fit digital dossiers. Solove argues that information collection for databases is not as strategic and centralized as one might think. Digital dossiers are assembled by a multitude of actors sharing data for a variety of purposes. In fact, the way they are described, one would think that digital dossiers come together by accident, a creation of chance unintentionally orchestrated by seemingly unrelated parties. For a more precise depiction of the loss of information privacy, Solove turns to the portrait of bureaucracy in Franz Kafka's *The Trial*, "where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process" (38). It is the vulnerability created by a system where decisions based on data may be made without our knowledge, say, or ability to challenge the outcome that is the crux of the problem. The shift from Big Brother to *The Trial* not only generates a more precise description of how digital dossiers are used and the impact this has on individuals, but it also refocuses attention on phenomena missed in other conceptual frameworks.

Using the concept of architecture in ways similar to Lawrence Lessig and Joel Reidenberg, Solove writes that privacy problems need to be understood structurally. Dealing with personal harm after a violation has occurred obscures the systemic nature of privacy loss. More attention should be directed toward the design of information networks, which have profoundly transformed relations between government, business, and individuals. Crucially, it isn't just the technology, "[the] law plays a profound role not just in solving the problems of digital dossiers, but in manufacturing them as well. The law is not merely reactive to new technologies that threaten privacy, but is also a shaping force behind these technologies as well as the amount of privacy we experience today" (224). In chapter's 6 and 11 Solove proposes a more robust legal architecture, one focused on regulating the institutional structures and relations responsible for digital dossiers.

Beyond a review of privacy law and the expansion of digital dossiers, the book's most powerful contribution may be found in the framework for situating these issues and proposals for confronting the loss of privacy. Rich with extensive examples, the book is highly recommended for readers looking for an introduction to information privacy as well as those already working on the problems created by digital dossiers.