PART II

IDENTITY

As Marsha Hanen points out near the end of Part I, new technologies that have the potential to rewrite what it means to be human will raise interesting questions about who we are and how we experience privacy. Part II picks up on those questions by interrogating various aspects of identity in a network society.

Steven Davis leads off with a philosophical analysis of the concept. He sets out a framework that distinguishes between metaphysical, epistemological, and social/cultural/political identities. In doing so, he sets the stage for those authors who seek to understand the ways in which demands for identity authentication implicate questions of power.

Charles Raab addresses this directly in his chapter. Like Davis, he sets out a top-level categorization of the concept of identity that accounts for both its individual and its social nature. He then examines the ways in which the social negotiation of both forms of identity is affected by the relative power status of the parties involved in the negotiation, particularly when misrepresentations of identity are perceived as inherently threatening to national security.

Michael Froomkin examines an instance of this same negotiation in the specific context of identity cards. He argues that residual romanticized notions of the American "cowboy" and the "Englishman" as a rights-holder have limited policymakers' ability to create an appropriate set of rules to protect privacy in light of new and emerging information technologies. He warns that greater transparency is required if we are to successfully build a broad bundle of rights into the identity card regime.

Jane Doe turns the tables, examining the social construction of the identities of women who have been raped and the manner in which they experience anonymity in jurisdictions that provide "protective" publication bans during and after the criminal trials of their assailants. She argues that court-enforced anonymity has identity implications for those who have been raped, with perils particular to racialized and other marginalized women. Sexually assaulted women are often identified as defiled and suspect; their lack of agency—indeed of any activity of their own—necessitates that their identities must be hidden and subsumed in the anonymity of being a Jane Doe. Her powerful interviews with women who have lived through this experience underscore the ways in which this identity fails to reflect the lived experience of these women as vibrant, reflective, and informed persons.

Jane Bailey examines what happens when a woman's private life is similarly taken out of context through self-exposure on the Internet. Her analysis of the experiences of Jennifer Ringley, the first woman to broadcast pictures of her daily life through a webcam, is a compelling account of the tension between the advancement of the feminist project and the reassertion of dominant representations of women as sexual objects. Although Ringley's experiment provided an opportunity to transgress and resignify sexual identities, Bailey ultimately concludes that the sexual imagery that Ringley broadcast was co-opted by and helped to reify the heterosexual male fantasy found in mainstream pornography.

David Phillips continues to interrogate questions of social justice in his analysis of the ways in which ubiquitous computing will restructure the social practices that we rely upon to construct our identities. He suggests that the notion of semiotic democracy would better inform policies intended to ensure that the resources for social meaning-making are equitably distributed in the network society.

David Matheson examines what happens when automated identification systems sidestep the careful negotiation of identity to which Phillips alludes. He argues that the nonreflexive nature of identifying oneself in an automated system invades privacy in the same way that Goffman's total institution does, by transforming social interaction into exercises of nonselective self-presentation. By depersonalizing those persons who are authenticated by the system, the system itself shrinks the opportunity for us to develop a robust dignity.

Ian Kerr raises similar concerns in the context of human-implantable radio frequency identification (RFIDs). He argues that the emerging RFID-enabled Internet of Things may soon become an Internet of People, and warns that a human-machine merger will challenge our notions of identity and privacy in a profound sense. Although the current regulatory regime provides some level of protection from today's one-off RFID applications, Kerr urges us to be forward thinking and to avoid sacrificing our core values in favor of the short-term expediencies of RFID-enabled networks.

In her examination of biometric identification as a form of border control, Shoshana Magnet reminds us that the human-machine merger is not neutral but works to perpetuate inequalities. Her analysis of the U.S.-Canada border demonstrates that biometric technologies imbue bodies with racialized and gendered meanings that continue to disadvantage some people and privilege others. Like Kerr, she warns that we must go beyond simplistic narratives of technology as neutral and efficient in order to fully understand the social consequences of the network society.

Gary Marx examines countervailing narratives of social resistance in his analysis of surveillance songs. He argues that popular music is a form of soul training that provides us with a source of imagery, which works to either deconstruct or legitimize the surveillance society. He identifies two opposing trends. On one hand, proponents of surveillance—control agents and members of the surveillance industry—represent surveillance as a means of solving serious social problems. Artists, on the other hand, tend to portray surveillance as the problem, and their songs warn us that the technologies upon which we rely may profane our experience as humans.

Jeremy Clark, Philippe Gauvin, and Carlisle Adams take social resistance to the network level. In order to promote technologies that support and protect autonomous action from state interference, they have devised a method to prove that an anonymous remailer is not the original sender of illegal material and is therefore not subject to search warrants. Their system is a practical attempt to push back against the current "is-ism"—the mistake of confusing how something is with how it must be—against which Lawrence Lessig warns.

Similarly, Daniel Howe and Helen Nissenbaum set out a technical method to hide one's surfing patterns from surveillance. Like Clark, Gauvin, and Adams, they argue that this kind of technology enables us to resist network surveillance on a principled basis, to protect the free inquiry, association, and expression that is an essential part of democratic citizenship. From this perspective, anonymity—the subject of the last section of the book—is a vital component of a network society that retains opportunities for individuals to enjoy privacy and to act autonomously.