sible the transformation of any organization into a conversational firm. Yet she cautions against overgeneralizations: ultimately, the future of this model of organization depends on the willingness of corporate leaders to support truly open and honest dialogue since new technologies do not carry an inherent capacity for positive transformation. Nowadays, when many organizations (political or otherwise) have learned to use social media as a tool to disseminate "alternative facts" rather than to promote openness, this lesson is more crucial than ever.

Hacked: A Radical Approach to Hacker Culture and Crime. By Kevin F. Steinmetz. New York: New York University Press, 2016. Pp. xv + 285. $89.00 (cloth); $28.00 (paper).

Kristi Brownfield
Northern State University

In the last 70 years, computers have become a fundamental part of our social, political, and economic landscapes. This machine explosion has inevitably spawned several different new social communities based on technology and the internet, such as fan communities, gaming communities, or hobbyist groups. One of the most misunderstood technology-focused communities is the hacker community. In *Hacked: A Radical Approach to Hacker Culture and Crime*, Kevin Steinmetz tries to scratch the disparate surface of a community that is often reviled and scrutinized as deviant or even criminal.

Steinmetz divides his book into two parts and centers his analysis specifically on political economy. The first half of the book is a fairly standard ethnography; Steinmetz uses data collected from in-depth interviews, participant observation at local hacker meet ups and conventions, and an extensive content analysis of 10 years of hacker publications. Steinmetz uses this data to deconstruct common depictions of hackers and reconstruct a more accurate picture of white, male, middle-class, technologically oriented problem solvers who value efficiency and skill in finding solutions, similar to what other researchers have found. Despite the unsurprising data, Steinmetz uses what he collects in a clever way by characterizing hackers as skilled craft workers. Steinmetz argues that "hacking as craft" is a skill developed over time and requires dedicated labor and investigation to master computers and code. Similarly, he describes the structures within the broader hacking subculture as a guild, encouraging social learning and the sharing of knowledge for the betterment of the community. Steinmetz then illustrates the hacking community's distrust of authority and their disdain of institutions as vehicles for control through surveillance and secrecy.

The second half of *Hacked* is built on the empirical data presented in the first half of the book. This is where Steinmetz largely crafts his theoretical argument regarding the political economy of hacking and hackers. In the

fourth chapter, Steinmetz argues that the conceptualization of hacking as craft encourages hackers not only to hack for profit as part of their occupation but also for leisure. While they may tackle different problems in their leisure hours, much of what hackers learn is also useful in their jobs. This blending of labor and leisure allows for exploitation of hacker talents by the companies and organizations for which they work. Steinmetz also argues that while hackers derive pleasure from the act of problem solving inherent in hacking, companies are able to further exploit the skills hackers develop by the "devaluation of skill" (p. 148). Since the labor of hacking cannot be automated, companies exploit that labor through the devaluation of skills—something to which hackers specifically contribute. The innovations and advances honed during their leisure time subsequently makes professional skills obsolete, forcing hackers to continually update their knowledge base to remain competitive and so that their skills remain current and their labor is not devalued. This situation is further exacerbated by the use of free and open source software such as Google's use of a streamlined version of the operating system Linux for their Android phones. Steinmetz points out that even hackers who participate outside of the normative computer industries and participate in illegal activities have created a billion-dollar industry centered on computer security in response to their actions. While hackers continue to see themselves and their communities as a transgressive craft, which prizes elegance and efficiency that could be used for the betterment of society, hacking as an *industry* has firmly been coopted by capitalism.

The fifth chapter of the book again turns away from what had been a far more theoretical discussion of hacking labor to the broader social understanding of "hacker." Steinmetz uses the Marxist definition of ideology to describe the ways in which the identity and role of hacker has been socially constructed in ways that benefit the existing capitalist systems. By casting hackers as criminals, authorities have created a problem population that is subject to heavy social control; this social control inevitably benefits private corporations through the exploitation of copyright through laws such as the Digital Millennium Copyright Act, the image of the criminal hacker, and the labor of hackers. Steinmetz concludes the book with discussion of ways to move forward with policy suggestions such as reducing the emphasis on moral panic, further protecting individual privacy, and reconfiguring our copyright laws. Steinmetz does acknowledge, however, that many of these suggestions would often come at the expense of corporate profit and thus be hard to realize.

Overall, the book provides conceptually interesting insight to hacking as a practice and hacking as a community. However, the two-part approach leaves the book feeling unbalanced; the first part of the book relies heavily on empirical data while the second half of the book is almost purely theoretical and largely ignores the data covered in the first part. Further, as Steinmetz works hard to debunk the criminal image of a hacker in favor of a more realistic portrayal, he often belabors the point and only pays token attention to the problematic behaviors and practices that do occur or that

originated in the hacking community such as trolling, swatting, or doxing. While this presentation is somewhat problematic, it is Steinmetz's ability to contextualize hacking within the political economy and to bring a critical Marxist perspective to hacking as labor, the reconceptualization of hackers as "crafty," and his discussions of the exploitation of the image of hackers and hacker labor that are by far the strongest points of *Hacked*. Steinmetz provides a provocative approach to understanding hacking, hackers, and the place of hackers within the larger U.S. economy through this framework, and he gives ample support for his approach that other researchers could easily use to further our empirical understanding of hacker as identity and hacking as practice.

Caught Up: Girls, Surveillance, and Wraparound Incarceration. By Jerry Flores. Oakland: University of California Press, 2016. Pp. vii+189. $29.95 (paper).

Kerryn E. Bell
Eastern Washington University

Increased concern exists in the United States over a possible school-to-prison pipeline. Jerry Flores furthers this argument in his book *Caught Up: Girls, Surveillance, and Wraparound Incarceration*. Through ethnographic research in Los Angeles, California, he argues that surveillance techniques in schools today resemble those of lockdown facilities such as prisons. His book provides an important contribution to the discussion of a school-to-prison pipeline by specifically focusing on Latina girls. Thus, Flores looks at the school-to-prison pipeline through the lens of intersectionality of gender and race/ethnicity.

Over a 24-month period, Flores conducted ethnographic research at two sites in Los Angeles: the El Valle Juvenile Detention Facility (El Valle) and Legacy Community Day School (Legacy). Community day schools in California are the newest version of alternative or continuation schools. His research included participant observation, eight focus groups, and 44 in-depth, semistructured interviews with incarcerated girls, teachers, administrators, counselors, probation officers, and teaching assistants. While he attempted to interview corrections officers, those attempts were unsuccessful.

In his book, Flores discusses how young Latinas first come in contact with the criminal justice system, how they are treated while in detention and the community school, and the link between these two institutions. His work is novel, as he explores how race, class, gender, and sexuality shape these girls' experiences. Sadly, Flores documents how linking El Valle and Legacy, in an attempt to provide wraparound services, actually resembles "wraparound incarceration." He suggests that through wraparound incarceration these girls cannot escape formal detention surveillance even after leaving the actual detention center.