particularly to treat people with symptoms from post-traumatic stress disorder (Regalado 2014).

In 'My brain made me do it! Neuroscience, criminal justice, and media', Emilia Masumeci details what she refers to as neurocriminology, a field that looks at how brains become issues on the witness stand during criminal trials, and she makes note particularly of those that have occurred in Italy and the United States. According to Masumeci's discussion regarding one intervening expert witness Kent Kiehl, a controversial neuroscientist from the University of New Mexico, all the criminal psychopaths that the researcher has studied appear to have brains that – like those of serial killers – differ from those of other people, in that the paralimbic system is too underdeveloped or the connection between the limbic system and the prefrontal cortex is missing. In any case, the author argues convincingly that by using neuroimaging in such cases to show the public just how the brain works, 'the media are contributing to the complex mechanism of "neuromanic imperialism" that is grotesquely simplifying and degrading humanity to mere neuron movements' (156).

In short, there is something in this volume for everyone interested in 'neuromediation', or the intersection of media study and the brain. In this regard, Michael Grabowski has not only done a great service to our field in furthering this sphere of enquiry, but also in demonstrating the relevance of media ecology to the neuroscientific endeavour. Hopefully the volume acts as a springboard for furthering this relevance and this research, and we can eagerly await the coming instalments.

REFERENCES

Girard, R. (1977), *Violence and the Sacred*, Baltimore: John Hopkins Press.

Regalado, A. (2014), 'Military funds brain-computer intefaces to control feelings', *Technology Review*, 29 May, http://www.technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/. Accessed 12 October 2015.

CODING FREEDOM: THE ETHICS AND AESTHETICS OF HACKING, E. G. COLEMAN (2013)

Princeton, NJ: Princeton University Press, 272 pp.,
ISBN: 9780691144610, Paperback, $27.95

Reviewed by Brett Lunceford, Independent Scholar

Hackers have long been a topic of interest for scholars of new media, and the idea of disrupting media systems is certainly nothing new for media ecologists. Still, some may question the subtitle of E. Gabriella Coleman's work, wondering whether there truly can be an ethical means of hacking, or where the aesthetics lie in tagging up websites. Coleman's book focuses not on the shadowy hackers found in movies and popular culture, but rather on the more

mainstream hackers who develop free and open-source software (F/OSS). Like others, Coleman distinguishes between hackers, who are those who work to refine and tweak code in inventive ways, and 'crackers' that break into computer systems illegally. However, as Coleman demonstrates in her case study of the controversy surrounding the creators of the DeCSS software and a PDF reader created to circumvent Adobe's e-book copy protection, the lines between legal hacking and illegal cracking are not always so clearly delineated.

Coleman opens with an extended discussion of how she shifted from academic observer to participant observer in the F/OSS movement. Here she also lays out her central claim that 'code is speech' (8). She then moves into a detailed history of the free software movement, reaching back into the age of bulletin board systems (BBS), the GNU Manifesto, and the origins of Linux. Coleman's anthropologist training comes out in her discussion of the social side of hacking found in various hacker conferences that draw participants from around the world. As Coleman moves into the legal dimensions of F/OSS, she details the shifts in how people think of software. As software became a closed, proprietary commodity, the F/OSS movement countered by opening their code to the user. She notes that code does more than create a piece of software that can be sold as a commodity; code, along with the copyright industries that control the code, shape what is possible. Despite the inroads that programs such as Linux have made in the computing world, Coleman suggests that the legal paradigm is slanted decisively towards corporate, proprietary software, especially with the passing of the Digital Millennium Copyright Act (DMCA).

In Chapter 3, Coleman attempts to define the values and characteristics of hackers. Many of these are no surprise to those who have done even a cursory read of previous work on hackers; she describes such attributes as cleverness, communal populism and individual elitism, and humour. However, I was surprised to see some omissions, such as Paul A. Taylor's (1999) *Hackers: Crime in the Digital Sublime*, which is one of the most extensive ethnographies of hacker culture to date. Perhaps this serves to differentiate between illegal hackers, which is the focus of Taylor's work, and the (mostly) legal hackers that Coleman examines, but these groups are not always mutually exclusive, and one may move from one group to the other. In Chapter 4, she puts this cultural analysis to work in exploring how these values shaped the development of Debian, a F/OSS Linux-based operating system. Coleman places this within the larger framework of social contract ethics, which I found to be an interesting means of analysis. Contrary to public perceptions of hackers as loners, the Debian project was a massive undertaking involving extensive cooperation among developers scattered around the globe. Because of its size and complexity, the need for a clear organizational structure was sometimes in conflict with the ideal of individuality. Coleman also demonstrates how these values led to a firm articulation of a moral stance from the Debian project.

The final section of the book more fully develops the argument that code is speech through case studies such as the DeCSS protests that used haiku to reveal decryption code and protests to free Dmitry Sklyarov, who wrote the program that unlocked Adobe e-reader files for Elcomsoft, his employer. In the case of Sklyarov, Coleman explores how hackers became increasingly politicized and took to the streets in protest with candlelight vigils and marches. Hackers in the underground had been political long before these events, but these accounts provide a greater depth to our understanding of

the political actions of hackers by describing the efforts of the mainstream hacker community. Just as every social movement has its radicals, there are also moderates agitating for change and much of the previous research has focused on those in the underground fringes, such as the Chaos Computer Club and Cult of the Dead Cow.

The main strength of this book, especially for media ecologists, is her central argument that code is speech. Coleman makes a convincing argument, but the implications for this claim are far-reaching and go well beyond First Amendment issues. For example, are there limits to what one can write in code? Can one write code that is obscene or incendiary? Are there differences in the kinds of code-speech that can be made by a corporate entity versus an individual? Who is ultimately responsible for corporate code-speech? How much change makes code a new work; can one remix or mash up code and make a new work? Is raw code different than compiled code? One may also consider the implications of what constitutes speech, especially in the wake of the *Citizens United* Supreme Court ruling that equated money with speech. If code can be considered speech, can blueprints, schematics, or even the frequencies that encode radio signals? In short, at which point can we say that the medium is not the message (apologies to McLuhan)? Another strength of this book is the skill with which Coleman examines legal structures surrounding information technology, often with an eye towards the absurdity of current regulations such as the DMCA. She notes that current regulations are skewed overwhelmingly towards corporate interests which, she suggests, is likely to stymie innovation and limit individual freedom. Finally, one could usefully view this book as a kind of continuation of Eric S. Raymond's (1999) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Coleman attempts to tell the story of those who live at the intersection of culture, law and code by living in their story. Although this results at times in a kind of romanticized view of the hackers she studies, she avoids the sensationalism found in many other books about hackers.

The main weakness of this text is what is omitted. Coleman seems at pains to distance the more legitimate hackers she studied from those who illegally break into computer systems, but in doing so she overlooks a significant body of literature surrounding hackers, most notably Taylor's (1999) ethnographic work. Coleman also slips between these two camps, illustrating the problem with placing hackers cleanly into one camp or the other. Still, this book would be of great interest to historians of technology and those interested in the mechanics of technological change.

REFERENCES

Raymond, E. S. (1999), *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, Cambridge, MA: O'Reilly.

Taylor, P. A. (1999), *Hackers: Crime in the Digital Sublime*, London: Routledge.