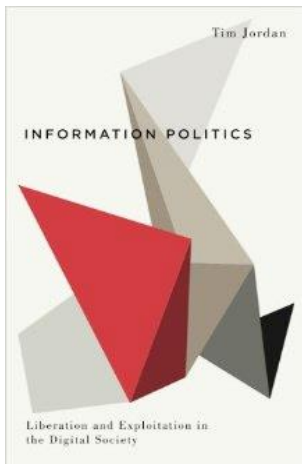Tim Jordan, ***Information Politics: Liberation and Exploitation in the Digital Society,*** London, UK: Pluto Press–Digital Barricades, 2015, 244 pp., $99.00 (hardcover), $23.23 (paperback).

Reviewed by
Nathalie Maréchal
University of Southern California, USA

In 2009, Tim Jordan wrote that "the possibilities for power and society in times of digital media and the Internet are still not well understood" (Jordan, 2009, p. 1). In Internet years, that may as well have been a lifetime ago. Six years on, such disparate and bewildering events as WikiLeaks (2010 and onward), the Arab Spring (2011), the Snowden revelations (2013), the hacking of Sony Pictures (2014), and most recently, the theft of unimaginable amounts of information on U.S. federal employees by (allegedly) Chinese hackers (2015) have given us a palpable sense of what is possible in this brave new digital world. Odds are there will be a new case to add to the list before this review is published. Meanwhile, governments, corporations, and civil society continue to spar, both publicly and behind the scenes, over trade-offs between privacy, free expression, public safety, and national security. Individuals, too, are embroiled in these politics of information, grappling daily with the intrusion of the digital into daily life at home, at work, and at play.

Tim Jordan's new book, *Information Politics: Liberation and Exploitation in the Digital Society*, explores the many ways that information—defined as "a difference that moves" (2015, p. 17)—is deeply enmeshed in modern life, starting with the assertion that "information as a politics of exploitation and liberation is now central to the twenty-first century" (2015, p. 1). Grounded in the work of canonical theorists such as Deleuze, Haraway, and Derrida, the book opens with highly theoretical musings on the nature of information and how it has been altered by computation. General audiences may be put off by the first part, clearly written with academics in mind; general readers would do well to skip to the second and third parts, which are empirically grounded, yet provide important insights into the emergent politics of information.

The book's three parts are further divided into three chapters each. Part I, "Theory of Information Power," opens with a deep dive into the concept of *recursion*, the property that uniquely pertains to information that is able to reflect upon itself and thus "eat itself" (2015, p. 29). This is (fittingly) a recurring theme throughout the book, and it is clear that Jordan has devoted a great deal of thought to this idea and its implications:

> With recursion we see massive flows of information that both are differences and return
> as differences, and hence as more information, which means that anyone who can

create a recursion can control the information that comes from that recursion; that is, information squatters are defined by the recursions they control. (2015, p. 64)

Chapter 2, "Technologies' Embrace," deals with the challenge of sifting through haystacks of information for the proverbial needle. Chapter 3, "Network and Protocol Theory: Dis/Organising Information Power," focuses on networks, or "the organisation of such recursions and devices into coherent and repeatable patterns of interaction between many kinds of actors—human, technological and other" (2015, p. 65).

In the second part, "Platforms," Jordan explores three important facets of the digital ecosystem: clouds (Chapter 4), the securitization of the Internet (Chapter 5), and social media networks (Chapter 6). The cloud, of course, refers to the ethereal "other place" where data is stored and from which it can be retrieved remotely through an Internet connection. As Jordan points out, the juxtaposition of "fluffy white clouds" and "arrangements of wires, radio-waves, computers, buildings and software" serves to pit "materiality against immateriality," obscuring "the cloud's dynamics of power": "clouds as a platform are both earthly and magical" (2015, pp. 83–84). Jordan uses the case of Megaupload to illustrate the ways that cloud platforms "create a means for cloud maintainers to benefit from free data that is collectively produced but can only be harvested by the cloud maintainer" (2015, p. 96).

Chapter 5 deals with securitization, a construct pioneered by the Copenhagen School of international relations, which emphasizes the rhetorical construction of existential threats by various actors in the international system, thus legitimating the use of force against these threats: "by saying 'security,' a state representative declares an emergency condition, thus claiming a right to use whatever means are necessary to block a threatening development" (Buzan, Wæver, & de Wilde, 1998, p. 21, cited in Jordan, 2015, p. 101). Securitization is thus closely related to Agamben's "state of exception," which "is not a special kind of law (like the law of war); rather, insofar as it is a suspension of the juridical order itself, it defines law's threshold or limit concept" (Agamben, 2005, p. 4, quoted in Jordan, 2015, p. 101). Jordan astutely notes that Agamben and the Copenhagen School both articulate "the paradox of state and government agencies that define a threat to be of such significance that to deal with it they suspend their own reason for existing" (2015, p. 102). He is of course referring to the assault on civil rights and liberties in the West in the aftermath of 9/11, typically justified as responses to the "four horsemen of the infocalypse": drug-dealers, money-launderers, terrorists, and pedophiles (2015, p. 104). Nation-states are far from being the only actors that engage in securitization processes vis-à-vis the Internet: For example, the emergence of a global digital rights movement is a testament to various groups' constructions of governmental crackdowns on Internet freedom as existential threats. In my view, this chapter stands out as the strongest in the book.

Part 3, "Battlegrounds," presents three case studies where "all these different dynamics and platforms [can] be seen in their complexity and messiness" (2015, p. 143): the iPad (Chapter 7), death in video games (Chapter 8), and hacktivism (Chapter 9). Chapter 7 considers "changes in working practices, the super-exploitation of global labour, gendered divisions in work, and environmental degradations" (2015, p. 143), four dynamics that are intimately connected to the rise of the global digital economy and that are poignantly illustrated by the production model of the iPad. Chapter 6, centered on what happens

when a player's video game avatar dies, illustrates the "connections between broad antagonisms of gender and race and those of information" (2015, p. 171). An avid gamer himself, Jordan is able to draw on his own experiences of watching his avatars succumb in ways that go beyond illustration and to share his essential insights.

The final chapter, "Hacktivism: Operation Tunisia, Modular Tactics and Information Activism" follows Anonymous' 2011 campaign supporting the Arab Spring in order to "demonstrate how information power can be examined and related to other forms of power" (2015, p. 176), building on Chapter 5's ("Securitisation of the Internet") study of political struggles over the new dynamics of power afforded by the Internet. Jordan traces the genealogy of hacktivism and hacking, starting with earlier waves of mass action hacktivism and digitally correct hacktivism [Jordan & Taylor, 2004, p. 69, quoted in Jordan, 2015, p. 185]), onward to the Zapatista movement of the 1990s and early 2000s, and finally drawing connections to the cypherpunk movement. He also links hacktivism to "the idea of leaking as a political act, again in the tradition developed early in online politics of seeing the Internet as a key arena for free flows of information" (2015, p. 189), exemplified by WikiLeaks and Snowden. As Jordan notes,

> information politics is here an activist politics in-itself . . . information politics provide tactics that may be taken up by nearly any struggle. . . . Understanding the nature of information as a political antagonism is then important for understanding the role of information in any political struggle in the twenty-first century. (2015, pp. 190–191)

This is an academic book of the highest quality that tackles what, in my opinion and Jordan's, is sure to be the defining struggle of the 21st century: the struggle for control over access to information. The first three chapters are most relevant to advanced graduate students and scholars, while the remaining chapters would appropriately serve as stand-alone reading assignments for undergraduate and graduate students. I noted earlier that chapters 5 and 9 were the strongest in my view, but chapters 7 and 8 (dealing with the political economy of the iPad and with death in video games) are also excellent, cogent overviews of their respective topics. Much like Jordan's 2008 book, *Hacking: Digital Media and Technological Determinism*, his *Information Politics* puts secondary sources in conversation with one another, synthesizing and situating them within and among several disciplinary traditions in the social sciences and beyond. This rapidly evolving field could use more books like this one.

References

Agamben, G. (2005). *States of exception*. Chicago, IL: University of Chicago Press.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis.* Boulder, CO: Lynne Rienner Publishers.

Jordan, T. (2008). *Hacking: Digital media and technological determinism*. New York, NY: Polity Press.

Jordan, T. (2009). Hacking and power: Social and technological determinism in the digital age. *First Monday, 14*(7). doi:10.5210/fm.v14i7.2417

Jordan, T. (2015). *Information Politics: Liberation and exploitation in the digital society*. London, UK: Pluto Press

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwar: Rebels with a cause*. London, UK: Routledge.