David Lyon, **Surveillance After Snowden**, Cambridge, UK: Polity Press, 2015, 120 pp., $45.00 (hardcover); $12.95 (paperback).

Reviewed by
M. M. Masoodi
Queen's University, Canada

David Lyon's latest book, *Surveillance After Snowden*, is an important addition to the field of surveillance studies in that it provides a comprehensive understanding of surveillance after the extraordinary revelations made by Edward Snowden in June 2013. The book is not about all the details of the revelations—that, of course, is not the point. Rather, the book places the Snowden revelations in context, with the aim of showing why Snowden's revelations are significant in how we understand surveillance today.

As a starting point, Lyon exposes the sociotechnical and political-economic conditions that have given rise to the specific kinds of surveillance we are experiencing in the 21st century. The significance of the transformation of new information technologies into surveillance tools is explored. For Lyon, what becomes strikingly evident during Snowden's revelations is what he calls the "three dimensions of surveillance" (p. 9) involving governments, corporations, and ordinary citizens. One, governments engage in mass surveillance of their own citizens—contradicting basic democratic practice. Two, corporations share their "own" data supplies (sometimes unwittingly) with governments to mutual benefit (corporations seek government contracts and governments seeks data). Three, ordinary citizens also participate in their own surveillance (although citizens are usually unaware of their participation in surveillance) through their online interactions—especially through social media and cell phone use (p. 9).

Lyon acknowledges that the aim of mass surveillance, as practiced by the NSA and revealed by Snowden, is to try to prevent crime and violence before it occurs. However, Lyon stresses that such practices raise real ethical concerns as they "suck innocent bystanders into the surveillance system in unconscionable numbers with dire results for human rights and civil liberties" (p. 11). Lyon explains in detail how this is done through "big data," or the linking and analysis of large data sets. For the author, big data has changed the character of surveillance we experience today and is responsible for the shift from targeted surveillance of groups and individuals to mass monitoring. Thus, when Snowden states that surveillance affects us all, it is no exaggeration.

The book provides a seamless and gentle road map showing readers how Snowden's revelations help us understand contemporary surveillance. I use the word "gentle" here because the book is written clearly and accessibly for a wide audience, including experts and nonexperts alike. Although theory is not discussed, underlying explanations are implied with an extensive list of notes to refer to.

In the first chapter, details of the Snowden revelations are provided, including descriptions of leaked programs such as X-KEYSCORE, Tempora, and PRISM that are operated by the NSA and its global partners. Chapter 2 examines how messages are intercepted and data gathered through cell phones and the Internet and also explores the consequences of these actions. What becomes clear here is the role of government agencies, private corporations, and the unwitting ordinary users. For Lyon, what holds these groups together, in a sense, is the software, the algorithms, and the codes that allow users' data to be systematically extracted, disclosed, and analyzed by various data gatherers. The next chapter hones in on the question of data—including metadata. Big data is "at the heart of the surveillance state revealed by Snowden" (p. 68). It is therefore no surprise that much of Lyon's focus is on what he calls "big data surveillance." As Lyon describes it, big data is constituted by a complex set of practices that are difficult to uncover and comprehend and yet practiced by all sorts of agencies, including government and commercial. It is this transferability of method from one field to another that is the problem, according to Lyon. Lyon describes how it is quite inappropriate and even risky when, for example, methods used by Amazon.com to suggest books or music to users are similarly applied by other agencies for other purposes, such as anti-terrorism. Big data could actually make some individuals more vulnerable as state authorities might make broad assumptions about them. Thus, there is the potential that these assumptions might produce negative real-life consequences for individuals. What comes next in chapter 4 is a discussion of privacy, human rights, democracy, and politics and what these actually mean today post-Snowden. Although Lyon suggests that these concepts are threatened by what Snowden has disclosed, in chapter 5 Lyon turns to a message of hope and urges readers not to frame the revelations in a negative or dystopian way, seeing only gloom and doom. What is instead recommended by the author is to turn to an ethical form of critique about big data surveillance and to envision a different kind of world— a world that we would like to see instead. From this vantage point, alternatives may be more clearly seen, discussed, and even implemented (p. 119).

It is important to note here that Lyon and other surveillance scholars have discussed many aspects of mass surveillance over the past couple of decades predating Snowden. However, according to Lyon, the Snowden revelations have provided "clear evidence" of mass surveillance happening, bringing concerns about mass surveillance to the public eye in ways never seen before.

Indeed, surveillance as described by Lyon is fluid (*liquid* to be more precise), constantly undergoing changes. It is currently morphing in several new ways, with this character change attributed to big data. According to Lyon, consequences of such changes (though difficult to predict precisely) include the intensification of pre-existing surveillance trends that rely on communication technologies through the expansion of interconnected data sets and analytical tools. Lyon describes three key ways in which these surveillance trends—enabled by big data—are intensifying: *automation*, an increasing reliance on software for surveillance; *anticipation*, focusing on future events and a quest for pattern-discovery; and *adaptation*, treating analytics as if methods can successfully be transferred from one field to another with little risk.

Most interesting for the reviewer is Lyon's description of where bulk data are obtained and aggregated. Using Rob Kitchin's work and applying it within the context of surveillance, Lyon describes three sources: directed, automated, and volunteered (Kitchin, 2014). Particularly intriguing is the third case. Data is "volunteered" by ordinary individuals through social media and the like "though their role is

hardly one of fully conscious actors in the drama" (p. 72). For Lyon, social media has boosted this "surveillance state" and are now the source of much data used not only for commercial purposes but also for so-called security.

A minor criticism here is a lack of exploration of the important and growing use of social media for security and intelligence, a phenomenon known as open source intelligence (OSINT), or to some, social media intelligence (SOCMINT). Even in its current form, though, Lyon's book is a treat for a broad audience interested in the impact of Snowden's revelations on surveillance. Indeed, there is a pressing need for everyone to understand surveillance because it truly affects us all. Lyon does an excellent job in presenting this clearly and accessibly, posing challenges but also presenting opportunities for hope.

References

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences.* London, UK: SAGE Publications.