Book Review

Review of Lennon, Brian. 2018. *Passwords: Philology, Security, Authentication*. Cambridge, MA: Harvard University Press.

232 pp. US\$43.50. Hardcover. ISBN: 9780674980761.

Mitch K. Jackson

University of Toronto, Canada
mitch.jackson@mail.utoronto.ca

Brian Lennon's *Passwords* offers a history for surveillance studies scholars who may be interested in the role of the digital humanities in developing the natural language processing tools that have become essential for security agencies across the globe. While a "history" may be a generous term (Lennon himself describes it as an "angular history"), the book offers a comprehensive overview of the convergence of not only cryptology and philology but also of the humanities and the surveillance state.

In the preface of *Passwords*, which reads as a confrontational polemic (taking on the financial crash of 2008, the security response to 9/11, Silicon Valley, MOOCs, and coding bootcamps amongst other targets), Lennon introduces the idea of an "academic surveillance complex" that is "actively or passively aligned with new modes of authoritarianism" (xi). One can look to any academic institution to see partnerships, either cemented or emerging, between security and academia. To offer one example outside of this book, at Carleton University in Ottawa, Ontario, a graduate program in "Infrastructure Protection & International Security" suggests future students should, according to the program recruitment copy, be "interested in asset protection and security, especially those responsible for the protection of critical infrastructures at all governmental levels and in private industry" (Future Students 2018). The program has been known to host events with titles such as "The Challenges of Dealing with Natural Resource Development Projects and Activism" that feature speakers from the security and intelligence community. As activism, specifically the expression of Indigenous sovereignty, is deemed a security threat inside academic institutions in direct conflict with their own promises to "decolonize" institutions, Lennon's claim of academic alignment with authoritarianism cannot easily be dismissed as hyperbolic.

For Lennon, this complex relationship was exposed via the Snowden leaks, which allowed for the suggestion that security had a massive role in transforming education by supporting any movement towards education that could lead to "defined technical applications" (viii). This is the point where "the social sciences and the humanities discovered the word 'digital', manufactured new troves of data and new tools for fooling with them" (ix). A critique of the digital humanities began to form in academic journals, centering primarily on the "ideological weight on the word 'digital'" (137), attempting to interrogate what exactly was meant by "digital" and what it was obfuscating.

The humanities is not the singular discipline embedded in this trend towards what van Dijck (2014) would term “datafication,” as every discipline in the academy had a pathway in which to reconnect (or perhaps connect) with the security state through the use of big data and other digital applications. But unique to the humanities is its long history of alignment with the surveillance state, “beginning with the direction of the First World War military cryptanalytic service units by scholars of the work of William Shakespeare” (xii). Lennon argues that there is a “structural alignment” between humanistic information retrieval, natural language processing, and the goals of the surveillance state.

In Chapter 1, which shares the same title as the book itself, Lennon offers his own “angular” history of passwords. Lennon reminds us that a “password provides effective security only to the extent that it is not a word... when it can no longer be found in a dictionary” (3). A strong password not only must meet the criteria of not being subject to dictionary-based attacks but also must be constantly changed in response to its degradation over time. Lennon also notes the increasing trend of information security becoming physical, where authentication is achieved through biometrics and physical tokens, “a development that may bring the linguistic, even literary history of account-based electronic access to an end” (12). For surveillance scholars, the most striking work in this chapter may be Lennon’s exploration of shibboleths, defined as “recognizable marks of communal membership ascertained through tests” (10). The shibboleth incident refers to a biblical passage in Judges 12 where the Ephraimites were challenged by the Gileadites to identify themselves by pronouncing “shibboleth.” Their pronunciation gave them away, and “we are told that the Gileadites slaughtered forty-two thousand Ephraimites on the spot” (13). For Lennon, this is where the “linguistic and literary history of the password begins” (12). This history of the shibboleth incident still extends to this today, with Lennon providing the compelling example of Australian government language proficiency tests, which are “less performance tests than means of detection and identification in border control” (14).

Chapter 3, “Machine Translation” historicizes the early work of machine translation while offering us hints at the academic rationales that allow for the justification of work with the surveillance state. These include the fight against ambiguity, the desire for social power and cultural prestige, the eternal calls to find one’s “niche,” and the neoliberal drive to make oneself and one’s work appear “useful” that are all clashing with the enticement and promise of resources and financial support from security agencies. For machine translation this came in the form of “generous government, military, and private funding” that was offered in order to advance Cold War geopolitical objectives (66).

The most appealing chapter for surveillance studies scholars is Chapter 5, “The Digital Humanities and National Security.” This is where Lennon fully connects back to his bombastic introduction, noting that this was the point where some academics began to realize that a new cryptophily “might owe as much to the conditions established by the security crisis of 2001 as to those established by the financial panic of 2008” (140). At this point, in the aftermath of the Snowden revelations, questions started to emerge about the noticeable absence of digital humanists in critiquing the surveillance state. Lennon quotes substantially from digital humanities scholars who wrote about sitting in on conference panels with non-descript members of the NSA and receiving offers to participate in projects funded by intelligence agencies as well as those who slowly began to realize the convergence of their own information collection practices and that of the intelligence community. Both institutions were interested in “the analysis of human behaviour, communication and networking patterns, semantic analysis, topic modelling...” (Mesiter qtd. in Lennon: 141). At all stages of data collection and processing, in both universities and security agencies, these data manipulation processes have been expanded through funding, increased computational power, and the offering of personal data from the users of social media. Both institutions tell us that these data produce some kind of useful knowledge, but the question of who that knowledge may be useful to is not fully addressed or acknowledged. For the digital humanities, this showcases the lack of consideration of the value inherent in their work.

This realization brought about key moments of ethical dilemma, such as the one posed by a group of digital humanities scholars in an article titled, “Is It Research or Is It Spying?: Thinking-Through Ethics in Big

Data AI and Other Knowledge Sciences.” The authors of the article considered the possibility that “our work and our students could be involved in the building of an unprecedented surveillance society” (Berendt, Büchler, and Rockwell qtd. in Lennon: 141). In analyzing this particular article, Lennon delivers a scathing critique, pointing out that the Snowden revelations forced these scholars to reconcile with the motives of their work, revealing that until that moment, “the new cryptophily that went by the name ‘digital humanities’ was flying blind” (142).

Lennon’s placement of the digital humanities as adjacent to the surveillance state fits in line with van Dijck’s (2014: 203) work on “datafication, dataism and dataveillance” where she finds that “all three apparatuses—corporate, academic, and state—are highly staked in getting unrestrained access to metadata as well as in the public’s acceptance of datafication as a leading paradigm.” Van Dijck (2014: 198) determines that “datafication as a legitimate means to access, understand and monitor people’s behavior is becoming a leading principle, not just amongst techno-adepts, but also amongst scholars who see datafication as a revolutionary research opportunity to investigate human conduct.” While van Dijck offers a broad critique of scholars who have been swept up in datafication, Lennon offers a deep examination of one specific scholarly field’s relationship with datafication, although without ever explicitly using that term. While the book may offer some fruitful contributions to this narrative, Lennon’s self-description of “angular” is incredibly apt. Excessive quotation (at one point, there are two pages of newspaper headlines in list format) takes away from the polemical punch and makes for tough reading at some points in the book. But for those who take joy in the critique of institutions and institutionalism, and the promise behind the word “digital,” there are corners worth peeking around.

References

- Future Students. 2018. Infrastructure Protection & International Security. <https://carleton.ca/ipis/future-students/> (accessed August 6, 2019).
- Van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.