Eric Schmidt and Jared Cohen, **The New Digital Age: Reshaping the Future of People, Nations and Business**. London, UK: John Murray, 2013, 337 pp., $17.96 (hardcover).

Reviewed by
Martin Hilbert
United Nations ECLAC
Pontificia Universidad Católica de Chile

Picking up *The New Digital Age: Reshaping the Future of People, Nations and Business*, written by two high-level Google executives in 2013, one might expect a collection of futuristic sci-fi speculations about the role of Internet-glasses, driverless cars, and holograms in the future of the U.S. consumer market. Instead, Eric Schmidt (executive chairman, Google) and Jared Cohen (director, Google Ideas) have written a book that is surprisingly political and refreshingly global in its perspective. The political perspective offered by these private sector executives provides the careful reader with the opportunity to glean interesting insights on delicate topics.
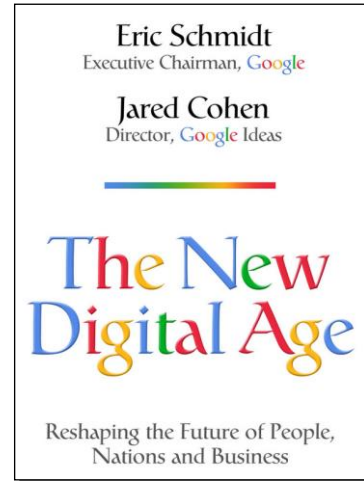
The chapters start with the common theme "The Future of . . ." and set a persistently geopolitical tone by focusing on ". . . Revolution," ". . . Terrorism," ". . . Conflict, Combat, and Intervention," and ". . . Reconstruction." Both authors had met four years earlier in Baghdad, while engaging in a discussion on how digital tools can be used to help rebuild a war-torn society. The write-ups of their joint experiences during many international trips and interviews—they include conversations with former U.S. Secretary of State Henry Kissinger, WikiLeaks founder Julien Assange, Rwanda President Paul Kagame, and Mexican billionaire Carlos Slim—are enjoyably readable and packed with anecdotes on how cyberspace and mobile phones transform security, privacy, and warfare. While the narratives do not lack the fanciful tone of Silicon Valley techies—for example, referring to mobile phone calendars as "memory prosthetics" and to online friendship networks as "social prosthetics" (p. 16)—for scholars who study the digital age, the book does not offer astonishing surprises or mind-boggling inspirations. Many scholars might wish that the authors had presented the same content in two-thirds of the book's 260 pages, as the redundant treatment of some recurrent topics in different chapters can seem overly repetitive at times.

For us, the main value of *The New Digital Age* is in the insights that the book offers into the minds, motives, and concerns of some of the leading private sector agents of change at the forefront of the digital revolution. The clarity of some of those stands is rather unexpected. While it is no surprise to re-encounter Google's well-known aversion to state- filtering interventions, it is thought-provoking to see the level of the authors' anxious anticipation of the fall of the entire Chinese political system due to its current Internet policy (pp. 147–148). It is interesting to find that the authors clearly draw limits to the power of the much-heralded digital tools, such as when they recognize that the reliance on digitally facilitated power of decentralized political movements is ridiculously naïve, as ". . . some sort of centralized authority must emerge if the movement is to have any direction" (pp. 129–130). In the light of

the PRISM surveillance scandal that was revealed only a few months after the publication of the book, some of the statements on privacy and whistle-blowing become particularly delicate in June 2013, when NSA whistleblower Edward Snowden accused Google, among other companies, of secretly cooperating with the U.S. government in spying on unsuspecting consumers.

It is instructive to hear about the clear disagreement of Google's leaders with the online transparency principles pursued by WikiLeaks when they lament that "Unfortunately, people like Assange and organizations like WikiLeaks will be placed to take advantage of some of the changes in the next decade" (pp. 41–42). While the authors repeat several times how important it is on us to "fight for our privacy or we will lose it" (pp. 173, 256), the authors also draw lines around the scope of this fight, as they argue that "security will always trump privacy concerns" (p. 175). They note that

> . . . a fully integrated information system, with all manner of data inputs, software that can interpret and predict behavior and humans at the controls, is simply too powerful for anyone to handle responsibly. Moreover, once built, such a system will never be dismantled. (p. 176)

This sounds almost identical to the conclusion of Snowden who testified in a June 6, 2013 video interview for *The Guardian* that "that's a dangerous capability for anybody to have," with the difference that he prefaced this sentence with these words:

> Companies like Google, Facebook, Apple, Microsoft, they all get together with the NSA and provide the NSA direct access to the back ends of all of the systems you use to communicate, to store data, to put things in the cloud, and even to just send birthday wishes and keep a record of your life. And they give NSA direct access that they don't need to oversee so they can't be held liable for it. I think that's a dangerous capability for anybody to have . . . (Poitras & Greenwald, 2013)

The authors show clear doubts about the effectiveness and stamina of the private sector in this battle when they note: "The only remedies for potential digital tyranny are to strengthen legal institutions and to encourage civil society to remain active and wise to potential abuses of this power" (p. 176). It is unusual to hear the omnipotent private sector calling for institutional oversight, as well as civil society oversight.

Regarding the style of argumentation in the book, slightly contradictory visions are naturally to be expected in a nonacademic, journalistic-style and futuristic book that consists of qualitative judgments and circumstantial evidence. The repeated vision of virtual statehood, like a virtual Kurdistan and Chechnya (pp. 101–102), contrasts with a potential vision of a "balkanization of the Internet" that mirrors existing nation-state power structures (p. 85). One overarching—and probably purposefully orchestrated—contradiction of the book consists of the futuristic vision of one single, tightly integrated physical and virtual world order versus a world that consists of two parallel physical and virtual domains. In their conclusions, the authors reveal that they see the latter hypothesis as more likely.

The extent to which *"The New Digital Age"* and its authors treat terrorism and cyber warfare (rather than focus on business, as promised in the subtitle) suggests that a large part of the book is more a product of Cohen's experience (as a former advisor to two secretaries of state, Condoleezza Rice and Hillary Clinton, as well as a member of the National Counterterrorism Center) than it is of Schmidt's. One section of the book might be read as an inspirational guide for cyber-terrorists as it explains how "hacking into the air-traffic-control system . . . [could] direct a large number of planes to fly . . . on collision paths" (p. 155), how "supervisory control and data acquisition (SCADA) systems . . . enable terrorists to . . . disable the heat-monitoring systems at nuclear power plants" (p. 156), and how "Afghans and Pakistanis will go to Europe to learn how to be cyber terrorists" (p. 165). The authors caution us that "some kind of coordinated physical and cyber attack is inevitable" (p. 156) and that "the target's ability to respond appropriately is compromised" (p. 165).

The expected commercial interests in a book written by private sector employees about the future of their sector are sometimes more obvious: for example, in the call for the installation of "plenty of bandwidth" (p. 251); the praise of cloud-computing as the silver bullet for a large variety of problems; or the repeated call for governments not to meddle with search engine results. Sometimes, commercial interests may make themselves apparent in the conspicuous omission of certain topics: For example, an entire section of the book paints a future picture of evil governments using online censorship to harass, repress and discriminate an unwanted minority by "simply eras[ing] content about that group from the Internet . . . similar to China's policy of active censorship" (p. 184).   Even so, the authors are aware that

> [E]xcluding oppressed populations from participating in the virtual world would be a very drastic and damaging policy, because in important ways they'd be left out and left behind, unable to tap into any of the opportunities for growth and prosperity that we see connectivity bringing. (pp. 185–186)

Nevertheless, the critical reader misses an equal discussion about how private sector interests are currently trying to diminish net neutrality, which would effectively exclude different socioeconomically disadvantaged groups from those same benefits in relative terms. The only mention of the concept (p. 93) consists of a quick remark about Chile, in 2010, becoming the world's first country to approve a law that guarantees net neutrality; there is no further discussion of the role of net neutrality for "The Future of . . .". Looking at the world through the lenses of an American technology provider also prevents the authors from counterbalancing their pervasive critical tone of Chinese domestic and foreign policies and of companies like Huawei with an equally critical view of American domestic and foreign expansion policies or of private sector failures: For example, see the one-sided discussion of the Chinese expansion into Africa (p. 111).

Overall, at times, some claims seem naïve: for example when Google executives argue that digital toys are an important force for good because their home entertainment potential distracts teenagers worldwide from joining terror groups (pp. 180–181). At other times, some generic judgments seem even dangerous: For example, in light of the Blackwater scandals and the disclosures of private sector employee Snowden, one would at least expect qualifications in a call (p. 204) for "military agencies and contractors to behave more like small private companies and start-ups (with maneuverability and the

option to move quickly)." Again, at other times, several arguments sound positivistic or simplistic to a social scientist, such as "Wire up the city, give people basic tools and they'll do most of the work themselves" (p. 180).

Despite all this, it nevertheless becomes clear that the authors are certainly not technological determinists. These self-declared "dry technology executive(s)" are well aware of their socially constructive power (p. 262). The motivation of these business executives "lies not in sci-fi gadgets or holograms but in the check that technology and connectivity bring against the abuses, suffering, and destruction in our world" (p. 257). From a romantic, glass-half-full perspective, this tells the tale of a geopolitically reflective technology provider that is here to stay with us through the good, the bad, and the ugly of technological revolutions. This is different from the pervasive tale of the unreflective engineers who built the atomic bomb by exclusively focusing on the technological possible, while neglecting the social impact. From a conspiracy-theoretic, glass-half-empty perspective, enough readers already allege that those statements are nothing more than plump, long-term marketing of their own commercial interest in line with the authors realization that "companies will be held responsible for destructive uses of their products" (p. 181). For example, see readers' comments on "Google Books" webpage. From a glass-half-full-and- empty perspective, we could interpret the reflections and concerns offered by Schmidt and Cohen as subjective contribution to a more civilized and sustainable model of technology-driven capitalism that requires open, public, and transparent debate. As the authors note, "Google, like many other companies, builds tools that anyone can use. Because of this, the company is continuously working to understand how to mitigate the risks that hostile individuals and entities will use these tools to cause harm" (p. 178).

Unavoidably, the authors use their own subjective definitions of "abuse," "suffering," and "destruction" (p. 181), as well as of "hostile individuals and entities" (p. 178). With books like these, though, the authors also venture into the public to share (some of) their views and offer us a platform to discuss and challenge them if necessary. The authors are correct when they note that there "is a canyon dividing people who understand technology and people charged with addressing the world's toughest geopolitical issues" (p. 9), and as social scientists, we know that bridging this gap inevitably requires the normatively biased social construction of technology. The multidisciplinary effort of Schmidt and Cohen is a pop science contribution that naturally comes with their own normative biases. While it is easy to critique the validity of their anecdotal evidence, the legitimacy of their simplistic pros and cons argumentation, and the biased subjectiveness of some of their claims, I view the book rather as an invitation, a challenge, and a contribution to an open debate. It is up to independent academic researchers—engineers and social scientists—to advance the discussion with their own strengths, including sophisticated analytical results that provide more objectively balanced perspectives through coherent, hard facts-based evidence.

References

Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. London, UK: John Murray.

Poitras, L. (Director), & Greenwald, G. (Interviewer). (2013, June 6). Edward Snowden interview-Part 2: The US government will say I aided our enemies. [Video Recording]. *The Guardian*. Retrieved from http://www.guardian.co.uk/world/video/2013/jul/08/edward-snowden-video-interview