This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Review - Black Code: Surveillance, Privacy, and the Dark Side of the Internet

https://www.e-ir.info/2016/03/18/review-black-code-surveillance-privacy-and-the-dark-side-of-the-internet/

SOPHIE BARNETT, MAR 18 2016

Black Code: Surveillance, Privacy, and the Dark Side of the Internet
Ronald J. Deibert
Signal: Nov. 2013

Ronald Deibert's *Black Code*, published in 2013, is an awakening read, vital to "anyone who cares about … civil liberties, crime and warfare in the digital age." It calls attention to critical concerns for international cybersecurity and offers tentative solutions. Deibert describes the paradoxical insecurity of cyberspace that results from unjustifiable and shocking government and civilian involvement, resulting in global "cyber phobia." This fear of vulnerability to cybercrime allows actors — hackers among them — to thrive on others' losses by breaking through firewalls, surveilling other computers, and downloading information. Today, nearly anyone can hack into a database. Internet censorship — attempted largely by democratic governments, ostensibly to protect citizens — is now a "global norm." Yet while *Black Code* successfully argues for the legitimate need of internet security, it fails to provide an equitable and practical solution.

Black Code acknowledges the inherent global nature of the internet, noting a lethal consequence: a loss of privacy and protection due to increasing pressures for government intervention. In using various platforms on the web, consumers are entrusting vast amounts of information to third party corporations, giving them inconceivable power. These third parties, including Skype, Google, Twitter, and Facebook, have access to alarming amounts of user information. Even more concerning is their use of this information. Deibert notes that governments increasingly pressure these corporations to censor or hand over information about their users. This became evident in the release of Google's biannual Transparency Reports, which revealed a "barrage" of government requests to remove content in an attempt to control content on the web.

Deibert holds that "the internet as we once knew it is officially dead." While extreme solutions aiming to "clamp down" on internet usage may seem viable, *Black Code* proposes something different. As open global communication is vital for the free exchange of ideas, measures protecting cyberspace freedom must be implemented without compromising its security. With civic networks at the forefront of his proposal, Deibert notes, "To protect planet Earth, we need to protect the Net."

Ronald Deibert is extremely qualified to speak in this area. Although advocating for stricter safety, Deibert strives to present a balanced viewpoint, acknowledging that the world wide web is an "open commons" allowing for the independent interaction of ideas and accumulation of knowledge — two vital components in human interaction — and stressing the need to keep this powerful mechanism open and protected. Referencing a combination of resources in supporting his call for an open, secure cyber community, Deibert cites direct source information, varying from terrorist groups like Al-Qaeda to Eugene Kaspersky, CEO of Kaspersky lab, a Russian-based research laboratory for cyber-security, and Richard Clarke, former National Coordinator for U.S. counterterrorism.

Deibert argues that while cyberspace will inevitably become securitized, consumers must determine the specifics and form. He proposes two core models to save cyberspace from deteriorating to "clean wars" – physically harmless

acts of sabotage in which no one dies. The models are: distributed security, consisting of structures overseeing cyberspace to secure users' rights and freedoms by holding actorsaccountable; and stewardship, a "planetary ecosystem in which no one central agency is in control," encouraging responsible behaviour online. While Deibert admits that his solutions for "corrective action" are challenging, he offers no insight into how these concepts could be successfully implemented. Furthermore, he downplays human motivation to find cures for society's ills. HIV/AIDS, a once fatal and entirely incurable disease, can now be managed because of human ingenuity. A solution for internet security may well be found the same way.

The first model remedy presented in *Black Code*, distributed security, is based on a structure that "rein[s] in and tie[s] down political power, both domestically and internationally," as a way to preserve the rights and freedoms of online consumers. Distributed security has three "key principles": mixture, division, and — most notably — restraint. Mixture and division are complements of each other, as mixture refers to intergovernmental cooperation and division the fact that no single actor being in control of others. Deibert supports this proposed solution with "multi-stakeholderism," whereby all actors are held equally accountable. He argues that participation of civilians is vital for the wellbeing of cyberspace, and that "governments and the private sector have more resources at their disposal than citizens … civic networks will need to collaborate to monitor all these centres of governance." Deibert does make an indisputable point — that citizens can never be in control of cyberspace as we do not possess the same level of knowledge, influence, or equipment as governments and the private sector. However, he provides no guidance in solving this imbalance and achieving his ideal of distributed security.

Deibert considers restraint the most consequential and vulnerable principle of distributed security and calls for a "reinforcement … of restraint on power," a need to oversee government agencies and corporations so that they do not misuse the personal information entrusted by consumers to third parties or commit "cyber espionage."*Black Code* suggests an implementation of a series of "checks and balances" to reduce the insecurity of cyberspace and thus increase transparency at the international level. That said, *Black Code's* principle of restraint is a sound idea lacking the practical aspects of how to guarantee the willingness of actors to comply, and how to select and train people for the jobs fundamental to this proposal. By extension, there would need to be an accountability mechanism for those those governing cyberspace.

Stewardship, the second model, requires cooperation from a variety of state and non-state actors. It "would moderate the dangerously escalating exercise of state power in cyberspace by defining limits and setting thresholds of accountability and mutual restraint." This solution focuses on "ethical behaviour" among consumers and would set standards in cyberspace etiquette that challenge those who do not comply.

While oversight bodies are critical components to stewardship in that they lead by example, Deibert argues that universities should act as the "ultimate custodians of cyberspace" because they serve as a medium between governments, who possess resources and knowledge, and average individuals, who do not. Protected by academic freedom and having vast access to resources, universities have incentives to "lift the lid" on cyberspace. However, with inevitable student turnover and constant budget cuts leading to increased dependency on funding from the private sector, how can this "special role" be sustained when it seems prone to corruption?

Black Code acknowledges the positive externalities of the internet era and explains the consequences of the many ways in which internet users voluntarily relinquish information. The last chapter of *Black Code* offers suggestions to protect the web, but they lack accountability and application. Relying on the honesty of administrators would not guarantee the security of cyberspace and will likely bring increased risk for users, as they will assume a safety that might not exist. As the need for cybersecurity intensifies, so too will the quest for solutions. To assume that solutions lacking today will not exist in the future ignores human ingenuity.

Black Code catalyzes the thinking about internet behaviour and security. Cybersecurity is a global issue that knows no borders. Any successful solution must therefore be global in practice. The rapid expansion of computer connectivity increases opportunities for criminal exploitation and cybercrimes can now be carried out within seconds to victims numbering in the millions. Given that some actors are less concerned than others, perhaps due to affordability or profit, securing cyberspace will not be an easy task. Therefore, understanding the travels of user data

is vital to consumers and does not necessitate an expertise in computer coding. Despite the increasing need for strengthening online control, restricting the openness of the web may destroy the basis for its popular existence. Deibert correctly notes that decisions regarding cybersecurity will strongly impact the future. Ultimately, as technology is constantly improving and societal norms are adapting to accommodate growth, internet usage is an inevitable forefront of the future. *Black Code* merely warns consumers not to take protection measures for granted.

Bibliography

"About the Author." *Black Code: Inside the Battle for Cyberspace.* Accessed October 20, 2014. http://blackcodebook.com/about.html#.VFaPeYcmbww.

"About the Author." Richard A Clarke. Accessed October 18, 2014. http://www.richardaclarke.net/bio.php.

"About the Citizen Lab." *Citizen Lab.* Accessed October 19, 2014. https://citizenlab.org/about/.

"Bio." *Citizen Lab. A*ccessed October 17, 2014. http://deibert.citizenlab.org/bio/.

"Book Review: 'Black Code: Inside the Battle for Cyberspace.'" *Frontiers of New Media.* Accessed October 16, 2014. http://www.frontiersofnewmedia.org/ronald-deiberts-black-code-inside-the-battle-for-cyberspace/.

Deibert, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto:McClelland & Steward, 2013.

Doctorow, Cory. "How to make cyberspace safe for human habitation." *The Globe and Mail,* May 30, 2013. http://www.theglobeandmail.com/arts/books-and-media/book-reviews/how-to-make-cyberspace-safe-for-human-habitation/article11990902/?page=all.

Khan, Saleem. "Book Review: Black Code, by Ronald J. Deibert." *National Post,* June 17, 2013. http://arts.nationalpost.com/2013/06/07/book-review-black-code-by-ronald-j-deibert/?__federated=1.

Meyer, Paul. "Black Code: Inside the Battle for Cyberspace." *bout de papier* 27*,* no. 4 (2013): 27. http://blackcodebook.com/docs/meyerreview.pdf.

Myers, Sara. "Review of Black Code: Inside the Battle for Cyberspace." *International Journal of Communication* 7 *(*2013): 1-3. http://ijoc.org/index.php/ijoc/article/view/2569/1043.

Slee, Tom. "Hacking Society: Three books look at the current state of play in the interconnected world."*Literary Review of Canada* 21*,* no. 7 (September 2013).

Thierer, Adam. "Book Review: Ronald Deibert's 'Black Code: Inside the Battle for Cyberspace'." *The Technology Liberation Front.* Last modified July 16, 2013. http://techliberation.com/2013/07/16/book-review-ronald-deiberts-black-code-inside-the-battle-for-cyberspace/.

"A Timeline of Aids." *AIDS.gov.* Accessed October 20, 2014. http://www.aids.gov/hiv-aids-basics/hiv-aids-101/aids-timeline/.

Torfing, Jacob. "Governance Networks." *The Oxford Handbook of Governance* (September 2012): 1-6. doi: 10.1093/oxfordhb/9780199560530.001.0001.

About the author:

Sophie Barnett is a second year, pursuing an Honours Bachelor of Arts degree in International Relations at the University of Toronto. Her primary research interests focus on cybersecurity and human rights, and how the two interact.