Black Code: How Advanced Technology is Destroying Privacy

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

2013, Toronto

ISBN: 978-0-7710-2535-8

Price: $11.84

303 pages

"We do know an awful lot these days, with data exploding all around us and information at our finger tips as never before. But the fact remains that nobody really knows where the dark forces in cyberspace are driving us, and whether they can be tamed. We can only keep probing beneath the surface, lifting the lid, and trying to get a handle on this domain that we have created, remembering that cyberspace is, after all, what we together make of it."[1]

Black Code, written by Ronald J. Diebert, is a terrifying read. Mr. Diebert could give Stephen King a run for his money; the only difference between the two authors is that Diebert's writings are one hundred percent non-fiction. This book discusses how the rapid changes in technology have created both ease and challenges for both individuals, and governments around the world. Diebert discusses how online privacy is becoming a notion of the past, and how 'hackers' are easily able to access both personal information from individuals, and classified

[1] Ronald J. Deibert, Black Code: Surveillance, Privacy, and the Dark Side of the Internet, 250 (2013).

information from governments. Diebert offers little solution to the hacking problem, but states what he believes the future holds involving this issue.

Ronald Diebert is a Professor of Political Science at the Munk School of Global Affairs, at the University of Toronto in Canada. He also is the Director of the Canada Center for Global Security Studies and the Citizen Lab. The Citizen Lab is an interdisciplinary lab that focuses on the advanced research and development of online security, human rights, and communication technology. Diebert has written numerous articles and books concerning technology, media, and world politics. He has also worked for numerous governments and organizations as a consultant on cyber privacy and cybercrimes. The author has also won numerous awards for his teachings and research, as well as receiving an honor from Queen Elizabeth for his work on protecting online privacy and security.

This book does not discuss specific laws per say, but focuses more on the privacy of both individuals and governments, and the crimes committed online that target specific individuals as well as governments across the world. Diebert is a Canadian citizen, but he does touch upon United States privacy protections, and how the average American citizen is increasingly growing concerned with their online privacy. Diebert discusses the Edward Snowden case, and how the former NSA contractor is wanted by the United States government for leaking confidential information, yet the NSA hasn’t been held liable for virtually cyber spying on American citizens. The author also touches upon Canadian privacy laws, and the laws of other nations he has worked with.

The book does not have the most cohesive structure, and has a bit of an odd breakdown of the sections in the book. Rather than discussing the hacking of governments and individuals separately, and the hacking by governments of its citizens as well as other governments, the book has no real order. The book would have made more sense if Diebert had sections placed together where he was talking about similar issues. Instead, the author first discusses his own experiences with investigating hacking of individuals (the Dali Lama) and how he has assisted governments (Canada and India) on dealing with hackings by other governments. To make the book more cohesive, Diebert should have broken each section down by topic, and then discussed his own experiences with the particular issue at the beginning or ending of the section.

On the side of the individual, Diebert discusses how the average internet user, which is increasing every day, is susceptible to having their private information compromised in numerous ways. He discusses how the average user can be hacked by unknown individuals, often residing in a foreign nation, and how these hackers are able to access all of the user's information through a simple virus. These viruses are extraordinarily easy to create, and can often be created after a simple google search. Through these viruses, they can either get to the user's banking information, or have full access to the user's computer.

The second manner in which an individual have their online privacy violated is through their own government. Diebert discusses the phenomenon of governments spying on their own citizens both in the United States and around the world. He specifically discusses the Edward Snowden leaks, and how the United States government is able to monitor citizen's phone use through metadata. Through this metadata, the government can see who the user has called, how the conversation has lasted, and where the call was made. Diebert also discusses how China is able to monitor their citizens online activity, and is even able to prevent those in the country from searching or accessing information. Through advanced programs, the Chinese government can prevent anyone in the country from searching information based on specific words, such as Tibet.

Governments have also been victim to hackers and the release of private and confidential information. Diebert specifically discusses how the Indian government contacted him personally for assistance after individuals in China (who they assumed were working for the government) hacked the Indian government's computer network. Through this hack, private government information ended up in the hands of another nation. Diebert also discusses how the United States has been hacked through numerous individuals who claim to be part of the hacktivist group 'Anonymous.' The group, which is made up of many unknowns, hacks all different people and organizations, including the United States government, when they feel that a wrong has been committed. The United States government and local governments have been hacked by Anonymous numerous times, and had classified and private information leaked onto the internet. Unlike hackings by foreign governments, members of Anonymous take credit for the hacks, and often make threats of more hacking if certain demands are not met.

Diebert does not offer a solution to the violations against cyber privacy or cybercrimes, but does discuss how through his personal experiences, he believes the future holds more of a threat. Both the individual internet user and governments need to be prepared for their private information potentially being breached. This book does not have a specific target audience, but can certainly be read by academics and those interested in internet privacy and security. Diebert writes the book through his personal experiences; the piece is readable, but could have been re-organized to have been read more clearly. The book is written clearly and logically, but should be re-organized by section to have a better flow. The author does a really good job explaining and supporting the propositions that he makes through examples. The author relies on himself as a source (through Citizen Lab) and government reports and data.

This book is an extremely valuable source to students, academics, and the average Joe who uses the internet. The author sought to explain and discuss the lack of privacy and security faced by many individuals and governments, and certainly succeeded. Though he does not offer a solution to prevent cybercrimes and the stealing of private information, he does warn of future breechings that are worse than the ones we face today. The major strengths of the book are that Diebert writes clearly enough that the average college student could easily understand what he is saying. The book is also exciting—which is rare for a non-fiction book about internet privacy. He is able write in a manner that the reader almost feels like they have first hand experienced the same events as Diebert. Although the book is thrilling, is does have a few minor flaws. The organization of the book is a bit scattered, instead of discussing each topic together, the placement of the sections should have been more thoughtfully placed.

Overall, I very much enjoyed this book. Ideally, I would recommend this book to any person who uses the internet. What Diebert has laid out in his book concerning internet privacy, and how little privacy there is terrifying. Those who have any personal information on the internet, including their banking information, email accounts, social media, or even just one who occasionally browses random websites should know that their data isn't secure. After reading this book, the reader would then understand why being vigil online is so important. I personally have always been skeptic about actual privacy on the internet, and believed in some form of government spying; this book has convinced me that I should probably be wearing a tinfoil hat. Ten out of ten would read again.