MARC GOODMAN, FUTURE CRIMES: INSIDE THE DIGITAL UNDERGROUND AND THE BATTLE FOR OUR CONNECTED WORLD (2016).

Anchor Books, 2016
ISBN: 978-0-385-5390-1
Price: $13.99, pp. 392

Reviewed by Susan Allen
Journal of High Technology Law
Suffolk University Law School

Future Crimes: Inside the Digital Underground and the Battle for our Connected World

How hard is it to break into the average computer system? Laughably easy. According to the Verizon study, once hackers set their sights on your network, 75 percent of the time they can successfully penetrate your defense within minutes.[1]

Introduction

Marc Goodman's *Future Crimes: Inside the Digital Underground and the Battle for our Connected World* provides readers with a comprehensive overview of the endless dangers that threaten society through its dependence on technology, social media, and the World Wide Web. Goodman introduces readers to the dark side of our connected world and alerts them of the risks they take just through the everyday use of smartphones, computers, televisions, and countless other technological devices. Goodman uses a plethora of anecdotes and short stories as examples to demonstrate the gravity of the hazards that lurk in cyberspace. Goodman explains

> The more we plug our devices and our lives into the global information grid—whether via mobile phones, social networks, elevators, or self-driving cars—the more vulnerable we become to those who know how the underlying technologies work and how to exploit them to their advantage and to the detriment of the common man. Simply stated, when everything is connected, everyone is vulnerable.[2]

---

[1] Marc Goodman, FUTURE CRIMES: INSIDE THE DIGITAL UNDERGROUND AND THE BATTLE FOR OUR CONNECTED WORLD, 16 (2016).
[2] Marc Goodman, FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE, AND WHAT WE CAN DO ABOUT IT 2 (2016) (ebook).

Goodman utilizes this medium to not only provide a warning to all members of the technological world, but also as a tool to spark conversation and the formation of strategies to combat the darker side of technology.

About the Author

Marc Goodman is a *New York Times* Best-Selling author, global strategist, and consultant who has dedicated much of his professional career fighting crime in the physical world as well as in cyberspace. Once a street police officer, Goodman has worked as the futurist-in-residence with the FBI, the United Nations' Counterterrorism Task Force, NATO, the United States government, and Interpol.[3] He holds degrees including a Master of Public Administration from Harvard University and a Master of Science in the Management of Information Systems from the London School of Economics.[4] He has also served as a Fellow at the Center for International Security and Cooperation at Stanford University and is a Distinguished Visiting Scholar the school's MediaX Laboratory.[5]

Mr. Goodman is the founder of the Future Crimes Institute and is the Chair for Policy, Law, and Ethics at the Silicon Valley think tank Singularity University. Mr. Goodman's publications have covered a wide variety of emerging technology issues. He has published articles with *The New York Times, The Economist*, *Wired*, *The Atlantic*, *Harvard Business Review*, *Forbes*, Oxford University Press, Jane's Intelligence Review, and the FBI Law Enforcement Bulletin.[6]

About *Future Crimes*

---

[3] *See About Marc*, Marc Goodman *archived at* https://perma.cc/5TSP-K5AA.
[4] *See id.*
[5] *See id.*
[6] *See id.*

Future Crimes mainly discusses the risks associated with the use of the technologies that today's society takes for granted. The book starts off with the alarming saga of a Mat Honan, a reporter for the magazine *Wired.* In a matter of a few minutes, Honan's digital world fell apart as a teenager located halfway around the world hacked into his various items and accounts and erased "all of the data Honan had spent a lifetime accumulating."[7] Such data included not only treasured family pictures, but also eight years' worth of Gmail messages, work conversations, notes, and reminders. The hacker's onslaught did not end there, as Honan soon found both his Twitter and Amazon accounts in the hands of this merciless hacker. Goodman uses this unfortunate tale to delve into one of his main purposes in writing this book; to advise readers of the online threats that exist in cyberspace. Goodman focuses his work on technology law and its associated crime as well as how more traditional crime employs technology to commit illegal acts. In this regard, Goodman writes not only about the technological crimes that first come to mind, such as the hacking and stealing of trade secrets, but also the use of cellphones to detonate roadside bombs. Goodman's writing runs the gamut in his coverage of technology law and examines how the future will only feature an exponential growth in such criminal acts.

Goodman divides his work into three parts, each featuring a number of chapters focused on specific areas of how technology and the law are intertwined. The first nine chapters comprise Part I of Goodman's work and exist to familiarize readers with basic knowledge of technology's relationship with the law and vice versa. These early chapters first expose readers to the depths of their vulnerability and the threats they face in participating in seemingly ordinary acts such as owning a smartphone, using its applications, and surfing the Web. By explaining what goes on behind the scenes with these everyday applications and websites, Goodman demonstrates to readers that privacy is now a luxury of the past, never to be seen or heard from

[7] *See* Goodman, *supra* note 1, at 8.

again. He explains to readers how every inquiry they make on google or to Siri is stored and kept as personal data, which is then sold to other companies and used for advertisement, among other purposes. Goodman's fourth chapter is entitled "You're Not the Customer, You're the Product." This clever title drives home his main point that no one is immune from the data collection that accompanies nearly every internet or application action imaginable.

Part II of *Future Crimes* features six chapters devoted to providing readers with examples and explanations of how technology is used to commit crime. These chapters discuss not only how criminals employ technological techniques to commit their illegal acts, but also how criminals in the future will use the technology of tomorrow against the innocent people who are so inclined to purchase or download it. Goodman introduces the concept of "Crime, Inc." in these middle chapters, a conglomerate that while not officially incorporated nevertheless wreaks havoc on society through its ability to hack and bug physical devices and internet websites. Examples of such criminality exist in the teenager who was successfully able to hack into the software that orchestrates the Lodz, Poland tram system, and alter tracks causing trains to run into one another. Other examples exist in Goodman's discussion of the Silk Road internet network, an intangible location that offers visitors any illegal product, from drugs to weapons to hitmen for hire. Lastly, Goodman presents the alarming ability of hackers having access to the controls of medical devices such as pacemakers and insulin pumps through Wi-Fi connection. He explains that having such an ability would enable criminals to kill these devices' owners by altering settings catastrophically.

In Part III, Goodman suggests methods to combat future digital crimes and provides readers with strategies to use to better protect themselves from the dangers of the online world and the criminal masterminds that lurk there. He provides suggestions as to how one can better

protect herself while maintaining a presence in the digital world. Goodman also examines possibilities of tomorrow's technology and presents theories as to how crime in cyberspace will exist in the future.

Analysis of *Future Crimes*

Goodman uses his book *Future Crimes* as a medium to educate readers of the vast dangers that exist in the digital world and provide some guidance as to how one can protect herself from an attack in cyberspace. Mr. Goodman's approach to accomplish this goal is to provide readers with countless real-life examples of victims of digital criminal acts. Through the use of this method, Goodman writes an educational book that is for readers of all types, as we are all connected in the digital world in one manner or another. Since seemingly everyone in the developed world uses a smartphone, the internet, and social media these days, students, professors, lawyers, and academics would benefit from reading *Future Crimes*. Critics have gone to the extend to describe this book as a "must-read."

Goodman produces a work that is extremely readable and rather enjoyable. The book first provides a historical background about cyber threats, which allows readers to get a basic grasp of the grave status of the viruses and other dangers that exist in cyberspace. He does not get bogged down in technical terms or overly-complicated diction. He writes in a manner that is easily understood as the vocabulary does not require one to have a degree in engineering or computer science. Although the book is readable, it is not structured in a very organized fashion. While the author focuses his chapters on different topics, at times the book seemed to be a bit repetitive or redundant. The anecdotal stories were interesting nonetheless, but some of them seemed to be a repeat of a previous account. Despite these flaws, Goodman makes no faulty assumptions. He is clearly a very knowledgeable person and can be trusted for what he writes.

Because he is so educated on the dangers of the digital world, he is able to support his claims by producing examples for readers. These examples are the products of years of research and investigation into the dangers of cyberspace.

Evaluation

Goodman's work is a valuable contribution to the field because it is successful in effectively warning readers of the dangers and risks we face through today's technology and our subsequent presence in the digital world. He achieves what he sought to achieve as he captures the reader's attention with scare tactics and then uses stories of actual experiences to paint a picture of the reality of cyberspace. He is effective in that he writes in a style that is both captivating and informative, ensuring that readers not only obtain the information that he wishes to provide, but also enjoy the book as well. One major strength of the book is the author's ability to explain seemingly rather technical concepts in a manner that is easily understood by less than tech-savvy people. He also is able to write about cybercrimes in a style that makes them seem as exciting as more tangible crimes such as burglary or murder.

Another strength of the book is that the author is very informative about these topics thanks to the research he has personally done through his own organization. He has spent decades researching on the topics he discusses in the text. This perspective also enables the author to provide suggestions to readers as to how they can better protect themselves from these threats.

Conclusion

Overall, I enjoyed reading this book because the author successfully conveys his ideas and expertise into language and concepts that are easily understood by everyday people. Because Goodman uses short stories to inform readers of the dangers of the digital world, his

writing is very thought-provoking for readers as it creates a genuine curiosity to uncover of the outcome of these unfortunate victims of cybercrime. Another quality of this book is that it can be easily understood by all readers regardless of your expertise in technology. As a reader I particularly valued this trait of the writing. This is definitely an informative book, in fact I would argue that it is perhaps a bit too informative because it has the ability to alarm readers into a state of paranoia. Because of this book, I view my smartphone, internet use, and social media presence with a completely different perspective than previously. I will definitely be more cautious and mindful of what I do and how I act in the digital world. Because of these changes, I would argue that this book is very convincing in the material that it presents.

I would recommend this book to essentially everyone. As stated previously, today's society is dependent upon the internet and technology regardless of if we want to admit it or not. This book is truly an eye-opener in that it makes readers aware of just want type of danger they are in as smartphone and computer owner. Not only are we at danger because of our devices, but also through the countless accounts and profiles we maintain through the internet via social media and other websites. Since everyone has at the least an email account in this day and age, we are all at risk. In conclusion, I would recommend that students, professors, and legal professionals should all read this Goodman's *Future Crimes*.