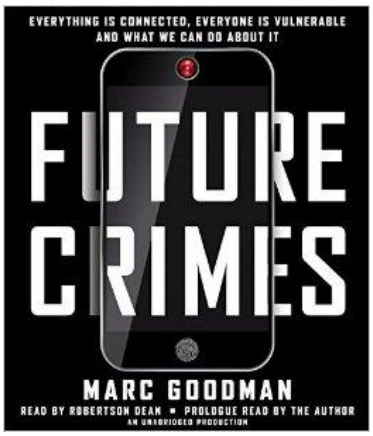
FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE AND WHAT WE CAN DO ABOUT IT



By: Marc Goodman
Bantam Press, RRP£20/Doubleday (2015);
ISBN-13: 978-0385539005, **ISBN-10:** 0385539002

464 pages; $27.95

Reviewed by: Alex Praschma

Journal of High Technology Law

Suffolk University Law School

"I study the future of crime and terrorism, and frankly, I'm afraid."[1]

In today's world, society has advanced in a multitude of respects thanks to our thirst for flourishing discoveries and technological innovation. Our lives are now surrounded by technology and impacted in ways that were once unimaginable. We look to technology for education, entertainment, traveling, creativity, and quite honestly, mere convenience in our everyday lives. However, this ever-expanding influx of technology is just beginning,

[1] MARC GOODMAN, FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE AND WHAT WE CAN DO ABOUT IT 2 (Doubleday 2015).

according to Marc Goodman, who says, "If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun."[2] While this seems exciting to the majority of our technologically dependent world, for global security experts like Marc Goodman, our society's blindness and addiction to technology is terrifying for reasons that are commonly overlooked.

Future Crimes: Everything Is Connected, Everyone Is Vulnerable And What We Can Do About It, is written by Marc Goodman, a global strategist and consultant, who has dedicated his career to the disruptive impact of technological advancements within our society, which affects security, business, and international affairs. Goodman holds a Master of Public Administration from Harvard University, as well as a Master of Science in the Management of Information Systems from the London School of Economics. Additionally, he has served as a Fellow at Stanford University's Center for International Security and Cooperation and is a Distinguished Visiting Scholar at Stanford's MediaX Laboratory. Goodman is frequently covered in the press, having been featured by CNN, ABC, NBC, BBC, Fox News, The Guardian, Le Monde and PBS, among others.

Over the past two decades of Goodman's professional career, he has accrued immense expertise in future security threats such as cybercrime, cyber terrorism, and information warfare while working with organizations such as Interpol, the United Nations, NATO, the Los Angeles Police Department, and the U.S. Government. Through these experiences, he has formulated insightful opinions and predictions about both commercial

[2] *See* Goodman, *supra* note 1, at 2.

and criminal enterprises, as well as how technology is continuously exploited conspicuously and in greater magnitudes than ever before.

Goodman begins his book by emphasizing that, "The technology we routinely accept into our lives with little or no self-reflection or examination may very well come back to bite us."[3] However, his message is not restricted to the past or even modern day technological misappropriation. Additionally, he jokes that his insights will not help you determine the adequate length for your Facebook password's security.[4] Rather, he discusses his own research and investigations with the LAPD, federal government, and international law enforcement organizations to illustrate how commercial and criminal enterprises have far surpassed the general public's awareness of their abilities.[5]

Specifically, both companies and criminals frequently utilize robotic, virtual reality, artificial intelligence, 3-D printing, and synthetic biology to scheme and achieve their desired end-results. Moreover, Goodman explains how we are a society continuing to construct ourselves with technological tools and how the very inventions we implement into our lives can easily be used against us.[6] In the eyes of Goodman, the bottom line is that innovation is generating extraordinary benefits while simultaneously making our society gravely vulnerable.[7]

In terms of commercial enterprises using technology to scheming against us, one extremely prevalent example is Goodman's discussion regarding social media privacy. To portray how companies are using innovative technology against us, Goodman claims that

---

[3] *See* Goodman, *supra* note 1, at 2.
[4] *See* Goodman, *supra* note 1, at 2.
[5] *See* Goodman, *supra* note 1, at 3.
[6] *See* Goodman, *supra* note 1, at 2.
[7] *See* Goodman, *supra* note 1, at 4.

if you ask the average Internet user why Google, Facebook, Twitter, YouTube, and LinkedIn are free, chances are that they do not know.[8] The majority of people tend to think that this has to do with advertising those annoying banner ads and pop-ups that never seem to go away. Nonetheless, this is exactly what these companies want consumers to think. While in reality, these products serve as tools to coax users into revealing incomprehensible volumes of data about themselves through a process called "data mining."[9]

Google, for example, created Gmail and provided users with high volumes of free storage. [10] In doing so, Google gained access to both personal and professional e-mails sent and received through Gmail. Goodman explains the discomforting impact through an eerie demonstrative, "If you wrote your mom an e-mail telling her you were sad over a recent break up, Google might suggest an antidepressant, a comedy club, or a Caribbean vacation."[11] As long as you are logged into Gmail, Google has ability track and profile you using your web searches. Today, Google arguably, "knows you better than you know yourself," and as a result, Google is consistently cashing in on your "top dollar" information by proceeding to sell your data profiles to advertising companies. To no surprise however, on numerous occasions, Google has been sued for privacy violations, security breaches, mishandling user data, theft of intellectual property, and contraventions of antitrust laws.

In 2012, Google was fined $22.5 million by the Federal Trade Commission for routinely circumventing privacy settings on Apple products by using the Safari web

[8] *See* Goodman, *supra* note 1, at 47.
[9] *See* Goodman, *supra* note 1, at 47.
[10] *See* Goodman, *supra* note 1, at 47.
[11] *See* Goodman, *supra* note 1, at 47.

browsers to track users' activities without their permission.[12] Just a year later in federal court, a judge denied a motion to dismiss a class action law suit against Google claiming that Google's practice of reading and mining Gmail users' e-mails violated U.S. laws against unlawful interception and wiretaps.[13] Similarly, Goodman asserts Facebook has also been sued repeatedly for privacy issues in federal court for "regularly and systematically intercepting users' private messages and sharing the data with advertisers and marketers."[14]

As Goodman insightfully points out, these large companies often win at the end, settling for pennies on the dollar for the information they have extracted from users. Thus, we are left wondering, "How are they getting away with this?"[15] In Goodman's very next chapter, he explains how ultimately, it's our own fault–we accept terms and conditions without even reading them. Yet, companies ensure that we are less likely to read them by making privacy policies an average length of 2,518 words long.[16] Companies who employ these terms and conditions, like Google, impose contractual language that is truly unreasonable and goes against users' best interests. Goodman says that according to Google's terms, "Anyone who uses Google Docs or happens to upload a spreadsheet, PDF, or Word document to Google Drive automatically grants ownership of the document to Google."[17] Here, Goodman does a superb job wielding one his examples by using world renowned, J.K. Rowling, as an example. Goodman claims that if Rowling were to have

[12] *See* Goodman, *supra* note 1, at 50.
[13] *See* Goodman, *supra* note 1, at 51.
[14] *See* Goodman, *supra* note 1, at 53.
[15] *See* Goodman, *supra* note 1, at 56.
[16] *See* Goodman, *supra* note 1, at 56.
[17] *See* Goodman, *supra* note 1, at 58.

written and uploaded *Harry Potter* on Google Docs, she would have granted Google the rights to her work and Google could theoretically (and legally) sell her stories.[18]

The information aforementioned is truly the tip of the horrifying iceberg that Goodman seeks to convey to his readers. Throughout the later chapters, Goodman tells numerous stories about how technology has been used for illegal activity ranging from cyber attacks and terrorism to theft and murder. From cyber gangs stealing two-third of American's credit card numbers and personal information to thefts of confidential U.S. Military plans, technology has been used to make criminal agendas much simpler to achieve and even harder to apprehend those behind them.

Goodman feels quite strongly about his fear of future technology quickly expanding. He predicts that the very tools used in these crimes will allow criminals to control aspects of our lives that are now connected to the internet, such as the ability to unlock our home's security system, and even the ability to change the setting of a pacemaker from untraceable locations afar.

One story that Goodman tells that exhibits not only the power of modern day criminals, but also our fearful dependence on technology, is an occurrence in California where over 450 criminals were accidentally released from prison after a system error conveyed incorrect information. Another took place in the United Kingdom where over 20,000 innocent citizens were wrongly branded as criminals and arrested on sight.[19] Goodman justifiably claims that our "trust in screens" is a giant red flag, as people no longer question the validity of what they see on their computer or IPhone screen.[20]

---

[18] *See* Goodman, *supra* note 1, at 59.
[19] *See* Goodman, *supra* note 1, at 135.
[20] *See* Goodman, *supra* note 1, at 140.

Consequently, the problems do not end here as various legal issues arise out of criminals' ability to commit heinous crimes across the globe. Issues in the realm of Jurisdiction often commence as a result of cyber terrorists committing crimes while located in other countries. These situations lead to drawn-out disputes between countries over who has the prevailing claim to prosecute the perpetrator once they are apprehended.

Goodman concludes his final chapters by making reasonable recommendations on how we as a society can protect ourselves, as well as remain informed about the risks associated with new age technology and innovation. His first critique revolves around his proposed strict liability laws for software companies by holding them liable for their products insufficient protection.[21] Frequently, software products are sold and distributed with "bugs" that are patched over and the problem is that hackers now have the ability to exploit this bugs in short increments of time, far before companies are able to remedy them. Essentially, Goodman believes that this would drive the software companies to provide stronger security and incentivize catching hackers.[22] He claims that by discarding ineffective passwords and implementing "multi-factored authentication" processes, the only people who would have the ability to read information sent over the Internet would be the intended recipient.

In respect to personal privacy and data, Goodman believes that in order for consumers to regain rights to their information from data collecting powerhouses like Google and Facebook, users will need to pay for the services using their money, rather than their data. Until this happens, consumers will continue to pay for services they wrongly assume are free with their personal data as currency. Additionally, such implementation

[21] *See* Goodman, *supra* note 1, at 385.
[22] *See* Goodman, *supra* note 1, at 385.

would reduce the risk of personal identification being made readily available to anyone with an Internet connection.

In terms of policing Internet crime, there is no solution that will solve it entirely. Rather, Goodman suggests that the best approach would be to increase government funding and recruiting of "hacking-experts" to law enforcement rosters.[23] In addition, Goodman suggests that a worthwhile investment would be to incorporate his concept, "*The Manhattan Project*," which is a team comprised of international cyber experts with the ability to not only secure criminal enterprises temporarily, but more so on a permanent basis.[24] Having such an implementation would theoretically allow us to not just catch hackers in the act, but also remain one step ahead.

Most importantly, Goodman's last piece of advice is an underlying theme that he threads throughout each chapter. The most practical approach to combating this nature of crime and protecting our individual livelihood is to increase awareness and remain informed about the risks associated with the gadgets we accept into our lives with open arms.

Overall, Future Crimes is an extremely fascinating reading for anyone. Goodman does an excellent job simplifying the processes and mechanics in way that allows the reader to understand how particular inventions put the user in grave danger. While he keeps things interesting, expect to remain on your toes, as the things he tells you range from the insecurity of our global network to hacker's ability to recreate your thumbprint on your new IPhone 6 "security scanner." If you take anything away from this book, you will surely think twice about how secure your phone truly is. One thing is for certain, if you choose

[23] *See* Goodman, *supra* note 1, at 383.
[24] *See* Goodman, *supra* note 1, at 388.

to read this book, you will never look at your phone, computer, or even car the same way– and honestly, after reading just one chapter of this book, you'll see why.

Vol. 59 No. 3. Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It. Intelligence in Public Media. Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It. Marc Goodman (Doubleday, 2015), 392 pp., index. Reviewed by Jay R. Watkins. The digital tidal wave is revolutionizing our lifestyles in many positive ways.Â And what about those Google cars plying the streets taking pictures at street view for Google Maps? They are also collecting IP addresses from mobile devices as they pass by. (107). And there is much more: the â€œInternet of Things,â€ the risks of wireless networks, drones, and devices to collect metrics about human behavior and bodily functions. (224â€“225; 248â€“252). Book Review by Canon Committee Member , Jon Oltsik: Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It (2015) by Marc Goodman. Executive Summary. Future Crimes by Marc Goodman details the dark side of technology, examining how new technologies are used and abused for criminal purposes.Â This analysis is especially useful for cybersecurity professionals seeking to understand what motivates cyber adversaries and how they do what they do. Goodman also does a good job of aligning cybercrime with the proliferation of Internet of Things (IoT) technologies.