CRIMINAL JUSTICE PRAXIS
Journal of OCCJE
Ohio Council of Criminal Justice Education • OCCJE.org

Citation: Merrill, Monica. 2015. "A Review of 'Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do about It'", Criminal Justice Praxis, Spring: 1-5.

Monica Merrill, Youngstown State University

Each page of *Future Crimes* drives home the author's point, that we are alarmingly unalarmed at how vulnerable technology has made us. Marc Goodman uses experience gained in his past position as the futurist in residence with the Federal Bureau of Investigations and current position as the Chair for Policy, Law and Ethics at Silicon Valley's Singularity University to discuss a variety of ways in which technology has already proven to not be as invincible as we would like to believe it is. He also discusses the ways technology has already been compromised and the effects it has had on society, and concludes with some recommendations for both society and the individual aimed at preventing, or at least managing, the relationship between technology and crime.

Goodman divides this text into three sections. The first focuses on ways in which technology and crime have already become intertwined. Here, he discusses the "borderless world" brought about by the advance of technology. Criminals now have the opportunity to commit international crimes from the comfort of their own home, while law enforcement agencies are often bound by national and jurisdictional concerns. The amount of information and services that are available online are ever increasing, but both

our laws and security technology can not keep up. This gap leaves the proverbial door wide open for criminals. The exponential growth of our use of technology as well as its advances, according to Goodman, is something that we have not devoted sufficient attention to.

The first section of the text also highlights the idea of big data, both collecting it and storing it. The author explains the ways in which companies collect data about you (cell phone apps, reward programs, etc.) and also explains that the data is bought and sold numerous times in order to serve multiple companies. Goodman elevates the discussion past the basic "if you don't have anything to hide, then why does it matter?" and answers this questions succinctly by pointing out that it is not the data collection that is the problem, but the fact that individuals have no control over their own data or how it is being used.

The second section of the book is fairly similar to the first. Goodman supplies more examples of crimes that have already been committed. For example, he cites cases where Square (a cell phone application which allows any user to charge a credit card) has been used to buy and sell illegal drugs. The use of Bitcoin, which allows the anonymous purchase of online services is also discussed as a way in which criminals are now able to "farm out" criminal acts that they may not have the skillset for. This opens up the pool of potential criminals from only those with the technological prowess to commit these types of crimes to anyone who can write up an ad on the dark web.

Not only does Goodman voice his concern about who will be able to commit these types of crimes in the future, he also discusses the ways in which our increasing willingness to engage the Internet of Things (IoT) may increase our vulnerability even

more. Things are increasingly more likely to have internet capabilities (automobiles, baby monitors, thermostats, refrigerators, pacemakers, prosthetic limbs, the list goes on). Since, as seen in the first section of the book, we already have trouble protecting and policing the things we already have online, Goodman sees this melding of the physical and virtual worlds as especially problematic.

He thinks up inventive ways in which the IoT can be used as a tool for criminals, but also ways in which it can be used as a tool for law enforcement. Each seem equally terrifying. For example, pacemakers which are connected to the internet are extremely vulnerable for hacking, leaving the gates wide open for targeted killing of a family member, stranger or political leader. The hacking of prosthetics also allows Goodman to explore the possibility of someone taking control of a person's internet enabled arm and having it do their bidding, whatever that bidding may be. To his credit, Goodman does point out ways in which regulatory agencies may be able to use the IoT to their benefit. For example, if the refrigerators in homes are internet enabled and catalog its contents, children's services can check to see if the refrigerator contains mostly formula or mostly beer.

The final, and shortest, section of the book discusses where Goodman thinks the technological component of crime is going and offers some prevention strategies. Here, he drives home an underlying message of the book: "the problem is not that technology is bad, but that so few understand it" (p. 351). He strongly advocates to eliminate technological illiteracy and for making legitimate opportunities more profitable to those who possess technological skills. He also proposes regulating software companies and holding them more accountable for their products, which necessitates that there are

people who understand this process to enforce it. He broaches interesting ideas about removing advertising as the main revenue generator for internet based companies.

Goodman offers a good deal of suggestions in the final section of this book, however he does not give many concrete or practical suggestions on how, exactly, to implement them. He says, "we will never solve 21st century problems with 19th century solutions" (p. 378), which is very true, however Goodman is light on the 21st century suggestions. He mentions some sporadic ideas about what we may consider (i.e., crowdsourcing cyber-security or encouraging pro bono coding) but does not really discuss how those ideas would be put into place. This is a shortcoming of the book.

An additional and related shortcoming is the disconnect between the title of the book and the text of the book. The title, *Future Crimes*, implies a discussion of where we think crime is headed, not where it has been. Although there are brief mentions of where technology can potentially take the criminal element in the future, there is more focus on crimes that have already happened than crimes Goodman thinks have potential to happen. The discrepancy between the title of the book and its contents should not take away from the valuable information and insight Goodman provides.

The biggest contribution of this book is the attention it brings to the vulnerabilities of our society. Goodman does an exceptional job of informing, even sometimes scaring, his reader. He calls for more focus on the ways in which our societal reliance on technology leaves us vulnerable to attacks from different angles, and with each example of a past crime he gives it will leave you wondering how we let things slide so long. Each example is shocking in its own right and will make you rethink your

relationship with technology. If the goal of this book was to draw attention to our current vulnerabilities I say it was a screaming success.

Future Crimes is a book that will appeal to anyone who has ever owned a smartphone. It is written in a very accessible way. Students, academics, practitioners "techies", and the general public alike would benefit form this text. There is something for everyone, and if the goal is to bring attention to our cyber vulnerabilities, the more who read it the better.

Reference

Goodman, M. (2015). *Future Crimes: Everything is Connected, Everyone is Vulnerable and What we Can do About it.* New York: Random House LLC.