Information is power. And in the Digital Age, information is everywhere. Data is stored in computers, smartphones, credit cards, cars, and television sets. Networking and bits control assembly lines, power grids, voting machines, medical devices, the planting and harvesting of crops. Metadata accumulates in the virtual warehouses of corporations and government agencies.

Connectivity, Susan Landau reminds us, has generated efficiencies and conveniences. It has also empowered organized crime hackers and nation-state attackers, who probe and penetrate “the soft underbellies of wired societies.”

In Listening In, Landau provides a sophisticated yet accessible primer on how communications technologies, devices, and services work; the threats to them; and the tools, including encryption, that, she maintains, can protect our privacy and secure our data.

Landau is extraordinarily well-qualified to address this subject. A professor in the School of Law and Diplomacy and the School of Engineering at Tufts University, she was a Senior Staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems. Landau is a member of the Cybersecurity Hall of Fame.

Listening In analyzes the most notorious acts of cyber exploits (theft of data) and cyber attacks (the destruction and disruption of machines). Landau’s accounts of North Korea’s hack of SONY Pictures, Russia’s destruction of Ukraine’s power grid, the insertion by the United States of the Stuxnet virus into Iran’s nuclear centrifuges, and the theft of Democratic National Committee emails, for example, highlight the targeting of “low-hanging fruit, introducing malware through the use of a known, but unpatched, vulnerability.”
She also notes that hackers often penetrate the systems of large corporations (which have improved security) by breaking into small companies which do business with them. Like so many cyber security experts, she warns users against choosing simple, easy-to-remember passwords. An application to routers, which allows a list of “trusted host” computers to access information without having to authenticate first, Landau adds, facilitates connectivity but makes it relatively easy for worms to propagate themselves from one machine to another without knowing each system’s log in.

Most important, *Listening In* illuminates the impact of digital technology on law enforcement. United States Attorney Preet Bharara, Landau reveals, used a text message – “do not buy plc m till I het guidance” – to get a conviction in a complex insider trading case. A generation earlier, that message might have been delivered over the phone, and lost to prosecutors. Khalid Sheikh Mohammed, the mastermind of the 9/11 attacks, was apprehended in Karachi, we learn, because he used the same SIM card on a slew of phones. And Bin Laden’s fear that his emails and phone calls could be tracked led him to communicate the old-fashioned way, by courier, a decision that enabled the United States to locate and kill him.

Acknowledging that officers of the law should seek access to evidence, Landau comes down decisively on the side of what she believes is society’s “desperate need” for communications and data security through “encryption without the possibility of exceptional access.” She insists that strong encryption supports public safety, national security and privacy. After all, secured devices have reduced crime and nation-state cyberattacks. Landau argues that despite the celebrated case of the iPhone used by San Bernardino terrorist Syed Rizwan Farook, which Apple refused to unlock for the FBI, law enforcement has an unprecedented array of tools available to it. And the existence of evidence has never meant that police, prosecutors, and federal officials should have unfettered access to it.

The debate, Landau concludes, should be about balancing easy access to data by law enforcement “with society’s need for strong online security.” It’s a debate we need to have.