**SIE 525 Information Systems Law**
Professor Harlan Onsrud

**Book Review Assignment**
**Potential Books to Consider**
**2017/2018**

**Acceptable Books for Review:**
The books as listed below are appropriate to read, summarize and review for the ***Book Review Assignment*** applied to Distance Students. The short summaries for each book listed below were drawn from Amazon.com or other Internet sources.

**Alternative Books:**
You may propose an alternative book to review if approved by the instructor. To gain such approval provide a similar citation (title, date and author) followed by a summary extracted from the web.

++++++++++++++++++++++++++++++

**CyberLaw: Text and Cases (2012)** 568 pages
Ferrera, Reder, Bird, Darrow, Aresty, Klosek, Lichtenstein
(https://faculty.bentley.edu/details.asp?uname=gferrera)
**Summary:**
This third edition guides readers through the complete business lifecycle--from idea to operation to dissolution--while examining the legal, managerial, and ethical issues affecting technology at each stage. Excerpted cases thoroughly explain the law in every chapter, while a running case about Google helps readers understand the real-world legal implications of operating a technology company today.

**Cyberlaw: The Law of the Internet and Information Technology (2012)**
Brian Craig (http://works.bepress.com/brian_craig/)
**Summary:**
Featuring the most current exploration of cyberlaw, *CYBERLAW* helps students understand the legal and policy issues associated with the Internet. Tackling a full range of legal topics, it includes discussion of jurisdiction, intellectual property, contracts, taxation, torts, computer crimes, online speech, defamation and privacy. Chapters include recent, relevant cases, discussion questions and exercises at the end of each chapter. Using a consistent voice and clear explanations, the author covers the latest developments in cyberlaw–from cases to legislation to regulations.

**Information Law: A compilation of articles Paperback (2016)**
By Peter Marx
Summary:
Who is liable for errors caused by information, information systems and digital media? Is there an effective way to address privacy and security when information can be accessed by anyone anywhere in the world? Attorney Peter Marx addresses these issues and many others in this compilation of articles. Information Law, a term Marx coined in 1985 has evolved into issues being addressed today within the fields of Internet law, Web law, cyberlaw and the law of digital media.

**Dark Territory: The Secret History of Cyber War (2016)**
Fred Kaplan (https://en.wikipedia.org/wiki/Fred_Kaplan_(journalist))
**Summary:**

“A consistently eye-opening history...not just a page-turner but consistently surprising.” —The New York Times

“A book that grips, informs, and alarms, finely researched and lucidly related.” —John le Carré

As cyber-attacks dominate front-page news, as hackers join terrorists on the list of global threats, and as top generals warn of a coming cyber war, few books are more timely and enlightening than Dark Territory: The Secret History of Cyber War, by Slate columnist and Pulitzer Prize–winning journalist Fred Kaplan.

Kaplan probes the inner corridors of the National Security Agency, the beyond-top-secret cyber units in the Pentagon, the "information warfare" squads of the military services, and the national security debates in the White House, to tell this never-before-told story of the officers, policymakers, scientists, and spies who devised this new form of warfare and who have been planning—and (more often than people know) fighting—these wars for decades.

From the 1991 Gulf War to conflicts in Haiti, Serbia, Syria, the former Soviet republics, Iraq, and Iran, where cyber warfare played a significant role, Dark Territory chronicles, in fascinating detail, a little-known past that shines an unsettling light on our future.

**Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage (2016)**
Gordon Corera (https://en.wikipedia.org/wiki/Gordon_Corera)
**Summary:**

The previously untold—and previously highly classified—story of the conflux of espionage and technology, with a compelling narrative rich with astonishing revelations taking readers from World War II to the internet age.

As the digital era become increasingly pervasive, the intertwining forces of computers and espionage are reshaping the entire world; what was once the preserve of a few intelligence agencies now affects us all.

Corera’s compelling narrative takes us from the Second World War through the Cold War and the birth of the internet to the present era of hackers and surveillance. The book is rich with historical detail and characters, as well as astonishing revelations about espionage carried out in recent times by the UK, US, and China. Using unique access to the National Security Agency, GCHQ, Chinese officials, and senior executives from some of the most powerful global technology companies, Gordon Corera has gathered compelling stories from heads of state, hackers and spies of all stripes.

Cyberspies is a ground-breaking exploration of the new space in which the worlds of espionage, diplomacy, international business, science, and technology collide.

**Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union (2016)**
Stephen Budiansky (https://en.wikipedia.org/wiki/Stephen_Budiansky)
**Summary:**

A sweeping, in-depth history of NSA, whose famous “cult of silence” has left the agency shrouded in mystery for decades

The National Security Agency was born out of the legendary codebreaking programs of World War II that cracked the famed Enigma machine and other German and Japanese codes, thereby turning the tide of Allied victory. In the postwar years, as the United States developed a new enemy in the Soviet Union, our intelligence community found itself targeting not soldiers on the battlefield, but suspected spies, foreign leaders, and even American citizens. Throughout the second half of the twentieth century, NSA played a vital, often fraught and controversial role in the major events of the Cold War, from the Korean War to the Cuban Missile Crisis to Vietnam and beyond.

In Code Warriors, Stephen Budiansky—a longtime expert in cryptology—tells the fascinating story of how NSA came to be, from its roots in World War II through the fall of the Berlin Wall. Along the way, he guides us through the fascinating challenges faced by cryptanalysts, and how they broke some of the most complicated codes of the twentieth century. With access to new documents, Budiansky shows where the agency succeeded and failed during the Cold War, but his account also offers crucial perspective for assessing NSA today in the wake of the Edward Snowden revelations. Budiansky shows how NSA's obsession with recording every bit of data and decoding every signal is far from a new development; throughout its history the depth and breadth of the agency's reach has resulted in both remarkable successes and destructive failures.

Featuring a series of appendixes that explain the technical details of Soviet codes and how they were broken, this is a rich and riveting history of the underbelly of the Cold War, and an essential and timely read for all who seek to understand the origins of the modern NSA.

*** Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It (2015)**[1]
Marc Goodman (http://www.marcgoodman.net/about/)
**Summary:**

One of the world's leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined.

Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation's power grid to air traffic control to financial services.

Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders.

With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, *Future Crimes* explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment.

*Future Crimes* provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, *Future Crimes* will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity—before it's too late.

**Cybersecurity and Cyberwar (2014)** 306 pgs
PW Singer and Allan Friedman (http://en.wikipedia.org/wiki/P._W._Singer, http://allan.friedmans.org/)

[1] * = highly recommended by past students

**Summary:**

A generation ago, "cyberspace" was just a term from science fiction, used to describe the nascent network of computers linking a few university labs. Today, our entire modern way of life, from communication to commerce to conflict, fundamentally depends on the Internet. And the cybersecurity issues that result challenge literally everyone: politicians wrestling with everything from cybercrime to online freedom; generals protecting the nation from new forms of attack, while planning new cyberwars; business executives defending firms from once unimaginable threats, and looking to make money off of them; lawyers and ethicists building new frameworks for right and wrong. Most of all, cybersecurity issues affect us as individuals. We face new questions in everything from our rights and responsibilities as citizens of both the online and real world to simply how to protect ourselves and our families from a new type of danger. And yet, there is perhaps no issue that has grown so important, so quickly, and that touches so many, that remains so poorly understood.

In *Cybersecurity and CyberWar: What Everyone Needs to Know®*, New York Times best-selling author P. W. Singer and noted cyber expert Allan Friedman team up to provide the kind of easy-to-read, yet deeply informative resource book that has been missing on this crucial issue of 21st century life. Written in a lively, accessible style, filled with engaging stories and illustrative anecdotes, the book is structured around the key question areas of cyberspace and its security: how it all works, why it all matters, and what can we do? Along the way, they take readers on a tour of the important (and entertaining) issues and characters of cybersecurity, from the "Anonymous" hacker group and the Stuxnet computer virus to the new cyber units of the Chinese and U.S. militaries. *Cybersecurity and CyberWar: What Everyone Needs to Know®* is the definitive account on the subject for us all, which comes not a moment too soon.

**Privacy: A Short History (2016)**
David Vincent (http://www.open.ac.uk/people/dmv33)
**Summary:**

Privacy: A Short History provides a vital historical account of an increasingly stressed sphere of human interaction. At a time when the death of privacy is widely proclaimed, distinguished historian, David Vincent, describes the evolution of the concept and practice of privacy from the Middle Ages to the present controversy over digital communication and state surveillance provoked by the revelations of Edward Snowden.

Deploying a range of vivid primary material, he discusses the management of private information in the context of housing, outdoor spaces, religious observance, reading, diaries and autobiographies, correspondence, neighbours, gossip, surveillance, the public sphere and the state. Key developments, such as the nineteenth-century celebration of the enclosed and intimate middle-class household, are placed in the context of long-term development. The book surveys and challenges the main currents in the extensive secondary literature on the subject. It seeks to strike a new balance between the built environment and world beyond the threshold, between written and face-to-face communication, between anonymity and familiarity in towns and cities, between religion and secular meditation, between the state and the private sphere and, above all, between intimacy and individualism.

Ranging from the fourteenth century to the twenty-first, this book shows that the history of privacy has been an arena of contested choices, and not simply a progression towards a settled ideal. Privacy: A Short History will be of interest to students and scholars of history, and all those interested in this topical subject.

**Intellectual Privacy: Rethinking Civil Rights in a Digital Age (2015)**
Neil Richards (http://law.wustl.edu/faculty/pages.aspx?id=314)
**Summary:**

Most people believe that the right to privacy is inherently at odds with the right to free speech. Courts all over the world have struggled with how to reconcile the problems of media gossip with our commitment to free and open public debate for over a century. The rise of the Internet has made this problem more urgent. We live in an age of corporate and government surveillance of our lives. And our free speech culture has created an anything-goes environment on the web, where offensive and hurtful speech about others is rife.

How should we think about the problems of privacy and free speech? In Intellectual Privacy, Neil Richards offers a different solution, one that ensures that our ideas and values keep pace with our technologies. Because of the importance of free speech to free and open societies, he argues that when privacy and free speech truly conflict, free speech should almost always win. Only when disclosures of truly horrible information are made (such as sex tapes) should privacy be able to trump our commitment to free expression. But in sharp contrast to conventional wisdom, Richards argues that speech and privacy are only rarely in conflict. America's obsession with celebrity culture has blinded us to more important aspects of how privacy and speech fit together. Celebrity gossip might be a price we pay for a free press, but the privacy of ordinary people need not be. True invasions of privacy like peeping toms or electronic surveillance will rarely merit protection as free speech. And critically, Richards shows how most of the law we enact to protect online privacy pose no serious burden to public debate, and how protecting the privacy of our data is not censorship.

More fundamentally, Richards shows how privacy and free speech are often essential to each other. He explains the importance of 'intellectual privacy,' protection from surveillance or interference when we are engaged in the processes of generating ideas - thinking, reading, and speaking with confidantes before our ideas are ready for public consumption. In our digital age, in which we increasingly communicate, read, and think with the help of technologies that track us, increased protection for intellectual privacy has become an imperative. What we must do, then, is to worry less about barring tabloid gossip, and worry much more about corporate and government surveillance into the minds, conversations, reading habits, and political beliefs of ordinary people.

A timely and provocative book on a subject that affects us all, Intellectual Privacy will radically reshape the debate about privacy and free speech in our digital age.

**Privacy in the Modern Age: The Search for Solutions (2015)**
Marc Rotenberg, Jeramie Scott, Julia Horwitz (Editors) (http://en.wikipedia.org/wiki/Marc_Rotenberg, https://www.linkedin.com/pub/jeramie-scott/2b/a86/516, https://www.linkedin.com/in/juliahorwitz)
**Summary:**

The threats to privacy are well known: the National Security Agency tracks our phone calls; Google records where we go online and how we set our thermostats; Facebook changes our privacy settings when it wishes; Target gets hacked and loses control of our credit card information; our medical records are available for sale to strangers; our children are fingerprinted and their every test score saved for posterity; and small robots patrol our schoolyards and drones may soon fill our skies.

The contributors to this anthology don't simply describe these problems or warn about the loss of privacy—they propose solutions. They look closely at business practices, public policy, and technology design, and ask, "Should this continue? Is there a better approach?" They take seriously the dictum of Thomas Edison: "What one creates with his hand, he should control with his head." It's a new approach to the privacy debate, one that assumes privacy is worth protecting, that there are solutions to be found, and that the future is not yet known. This volume will be an essential reference for policy makers and researchers, journalists and scholars, and others looking for answers to one of the biggest challenges of our modern day. The premise is clear: there's a problem—let's find a solution.

**Privacy Law Fundamentals, Third Edition (2015)**
Daniel J. Solove (https://en.wikipedia.org/wiki/Daniel_J._Solove) and Paul M. Schwartz (https://en.wikipedia.org/wiki/Paul_M._Schwartz)
**Summary:**

The third edition of the popular Privacy Law Fundamentals text incorporates extensive developments in privacy law and includes an introductory chapter summarizing key new laws, cases and enforcement actions. Privacy Law Fundamentals is no treatise-its accessible, portable format delivers vital information in a concise and digestible manner. It includes key provisions of privacy statutes; leading cases; tables summarizing the statutes (private rights of action, preemption, liquidated damages, etc.); summaries of key state privacy laws; an overview of FTC enforcement actions; and answers to frequently asked questions, including:

What are the key points in all the HHS resolution agreements for HIPAA violations?

What are the theories of harm in litigation for privacy and security cases and how well has each fared?

What are the most significant FTC privacy and data security cases of the past decade?

**Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (2015)**
Bruce Schneier (http://en.wikipedia.org/wiki/Bruce_Schneier)
**Summary:**

You are under surveillance right now. Your cell phone provider tracks your location and knows who's with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you're thinking because it saves your private searches. Facebook can determine your sexual orientation without you ever mentioning it.

The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we're offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches.

Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we've gained? In *Data and Goliath*, security expert Bruce Schneier offers another path, one that values both security and privacy. He shows us exactly what we can do to reform our government surveillance programs and shake up surveillance-based business models, while also providing tips for you to protect your privacy every day. You'll never look at your phone, your computer, your credit cards, or even your car in the same way again.

**Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are (2017)**
Seth Stephens-Davidowitz
**Summary:**

The basic thesis of "Everybody Lies" is that online data on human behavior, including Google searches and data from Facebook, shopping and pornographic sites, can reveal much about what we really think than data from surveys in which people might be too embarrassed to tell the truth. In our unguarded moments, when we are alone and searching Google in the privacy of our homes, we are much more likely to divulge our innermost desires. The premise is that truly understanding human behavior by way of psychology or neuroscience is too complicated right now, so it's much better to simply bypass that kind of understanding and look at what the numbers are telling us in terms of what people's online behavior. In doing this the author looks at a remarkable variety of online sources and studies by leading researchers, and one must congratulate him for the diversity and depth of material he has plumbed.

What has allowed us to access this pool of unguarded opinions and truckloads of data concerning human behavior is the Internet and the tools of "big" data. As the author puts it, this data is not just "big" but also "new", which means that the kind of data we can access is also quite different from what we are used to; in his words, we live in a world where every sneeze, cough, internet purchase, political opinion, and evening run can be considered "data". This makes it possible to test hypotheses that we could not have tested before. For instance, the author gives the example of testing Freud's Oedipus Complex through accessing pornographic data which indicates a measurable interest in incest. Generally speaking there is quite an emphasis on exploring human sexuality in the book, partly because sexuality is one of those aspects of our life that we wish to hide the most and are also pruriently interested in, and partly because investigating this data through Google searches and pornographic sites reveals some rather bizarre sexual preference that are also sometimes specific to one country or another. This is a somewhat fun use of data mining.

Data exploration can both reveal the obvious as well as throw up unexpected observations. A more serious use of data tools concerns political opinions. Based on Google searches in particular states, the author shows how racism (as indicated by racist Google searches) was a primary indicator of which states voted for Obama in the 2008 election and Trump in the 2016 election. That's possibly an obvious conclusion, at least in retrospect. A more counterintuitive conclusion is that the racism divide does not seem to map neatly on the urban-rural divide or the North-South divide, but rather on the East-West divide; people seem to be searching much more for explicitly racist things in the East compared to the West. There is also an interesting survey of gay people in more and less tolerant states which concludes that you are as likely to find gay people in both parts of the country. Another interesting section of the book talked about how calls for peace by politicians after terrorist attacks actually lead to more rather than less xenophobic Google searches; this is accompanied by a section that hints at how the trends can be potentially reversed if different words are used in political speeches. There is also an interesting discussion of how the belief that newspaper political leanings drive customer political preferences gets it exactly backward; the data shows that customer political preferences shape what newspapers print, so effectively they are doing nothing different from any other customer-focused, profit making organization.

…. etc.

**Information Privacy Fundamentals for Librarians and Information Professionals (2014)**
Cherie L. Givens (https://www.linkedin.com/in/cheriegivens)
**Summary:**

As more information is collected, shared, and mined, the need to understand and manage information privacy has become a necessity for information professionals. Governments across the globe have enacted information privacy laws. These laws continue to evolve and the information privacy protections that have been established differ by country. A basic understanding of privacy law, information privacy approaches, and information security controls is essential for information professionals to properly manage private/personally identifiable information (PII) in differing capacities in libraries, academic institutions, corporations, hospitals, and state and federal agencies.

Understanding and knowledge of applicable privacy laws and the ability to write privacy policies and procedures for the proper handling of PII are crucial skills for librarians and other information managers.

Information Privacy Fundamentals for Librarians and Information Professionals is tailored to the needs of librarians and information professionals. It introduces library and information professionals to information privacy, provides an overview of information privacy in the library and information science context, U.S. privacy laws by sector, information privacy policy, and key considerations when planning and creating a privacy program.

**Technocreep: The Surrender of Privacy and the Capitalization of Intimacy (2014)**
Thomas P. Keenan (no obvious website showing credentials)
**Summary:**

"Technology is rapidly moving into our bodies," writes cyber expert Keenan, "and this book gives a chilling look ahead into where that road may lead us – on a one way trip to the total surrender of privacy and the commoditization of intimacy." Here is the definitive dissection of privacy-eroding and life-invading technologies, coming at you from governments, corporations, and the person next door.

Take, for example, "Girls Around Me": a Russian-made iPhone App that allowed anyone to scan the immediate vicinity for girls and women who checked in on Foursquare and had poorly secured Facebook profiles. It combined this information in a way never intended by the original poster. Going to a Disney theme park? Your creepy new "MagicBand" will alert Minnie Mouse that you're on the way and she'll know your kid's name when you approach her. Thinking about sending your DNA off to Ancestry.com for some "genetic genealogy"? Perhaps you should think again: your genetic information could be used against you.

With security scares like the Heartbleed bug (which compromised even supposedly safe internet behemoths like Google and Yahoo!) becoming more commonplace, this book is a must-read for anybody who values their privacy in a wired world.

**Age of Context: Mobile, Sensors, Data and the Future of Privacy (2013)** 225 pgs
Robert Scoble & Shel Israel (http://en.wikipedia.org/wiki/Robert_Scoble, http://en.wikipedia.org/wiki/Shel_Israel)
**Summary:**

In 2006, co-authors Robert Scoble and Shel Israel wrote Naked Conversations, a book that persuaded businesses to embrace what we now call social media. Six years later they have teamed up again to report that social media is but one of five converging forces that promise to change virtually every aspect of our lives. You know these other forces already: mobile, data, sensors and location-based technology. Combined with social media they form a new generation of personalized technology that knows us better than our closest friends. Armed with that knowledge our personal devices can anticipate what we'll need next and serve us better than a butler or an executive assistant. The resulting convergent superforce is so powerful that it is ushering in a era the authors call the Age of Context. In this new era, our devices know when to wake us up early because it snowed last night; they contact the people we are supposed to meet with to warn them we're running late. They even find content worth watching on television. They also promise to cure cancer and make it harder for terrorists to do their damage. Astoundingly, in the coming age you may only receive ads you want to see. Scoble and Israel have spent more than a year researching this book. They report what they have learned from interviewing more than a hundred pioneers of the new technology and by examining hundreds of contextual products. What does it all mean? How will it change society in the future? The authors are unabashed tech enthusiasts, but as they write, an elephant sits in the living room of our book and it is called privacy. We are entering a time when our technology serves us best because it watches us; collecting data on what we do, who we speak with, what we look at. There is no doubt about it: Big Data is watching you. The time to lament the loss of privacy is over. The authors argue that the time is right to demand options that enable people to reclaim some portions of that privacy.

**The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies (2014)**
Erik Brynjolfsson (http://mitsloan.mit.edu/faculty-and-research/faculty-directory/detail/?id=22672)
**Summary:**

A New York Times Bestseller. A "fascinating" (Thomas L. Friedman, New York Times) look at how digital technology is transforming our work and our lives.

In recent years, Google's autonomous cars have logged thousands of miles on American highways and IBM's Watson trounced the best human Jeopardy! players. Digital technologies—with hardware, software, and networks at their core—will in the near future diagnose diseases more accurately than doctors can, apply enormous data sets to transform retailing, and accomplish many tasks once considered uniquely human.

In The Second Machine Age MIT's Erik Brynjolfsson and Andrew McAfee—two thinkers at the forefront of their field—reveal the forces driving the reinvention of our lives and our economy. As the full impact of digital technologies is felt, we will realize immense bounty in the form of dazzling personal technology, advanced infrastructure, and near-boundless access to the cultural items that enrich our lives.

Amid this bounty will also be wrenching change. Professions of all kinds—from lawyers to truck drivers—will be forever upended. Companies will be forced to transform or die. Recent economic indicators reflect this shift: fewer people are working, and wages are falling even as productivity and profits soar.

Drawing on years of research and up-to-the-minute trends, Brynjolfsson and McAfee identify the best strategies for survival and offer a new path to prosperity. These include revamping education so that it prepares people for the next economy instead of the last one, designing new collaborations that pair brute processing power with human ingenuity, and embracing policies that make sense in a radically transformed landscape.

A fundamentally optimistic book, The Second Machine Age alters how we think about issues of technological, societal, and economic progress.

**Who Owns the Future? (2014)**
Jaron Lanier (http://en.wikipedia.org/wiki/Jaron_Lanier)
**Summary:**

Jaron Lanier is the father of virtual reality and one of the world's most brilliant thinkers. *Who Owns the Future?* is his visionary reckoning with the most urgent economic and social trend of our age: the poisonous concentration of money and power in our digital networks.

Lanier has predicted how technology will transform our humanity for decades, and his insight has never been more urgently needed. He shows how Siren Servers, which exploit big data and the free sharing of information, led our economy into recession, imperiled personal privacy, and hollowed out the middle class. The networks that define our world—including social media, financial institutions, and intelligence agencies—now threaten to destroy it.

But there is an alternative. In this provocative, poetic, and deeply humane book, Lanier charts a path toward a brighter future: an information economy that rewards ordinary people for what they do and share on the web.

*** One World Schoolhouse (2013)** 259 pgs
Salman Khan (http://en.wikipedia.org/wiki/Salman_Khan_%28educator%29)
**Summary:**

A free, world-class education for anyone, anywhere: this is the goal of the Khan Academy, a passion project that grew from an ex-engineer and hedge funder's online tutoring sessions with his niece, who was struggling with algebra, into a worldwide phenomenon. Today millions of students, parents, and teachers use the Khan Academy's free videos and software, which have expanded to encompass nearly every conceivable subject; and Academy techniques are being employed with exciting results in a growing number of classrooms around the globe.

Like many innovators, Khan rethinks existing assumptions and imagines what education could be if freed from them. And his core idea-liberating teachers from lecturing and state-mandated calendars and opening up class time for truly human interaction-has become his life's passion. Schools seek his advice about connecting to students in a digital age, and people of all ages and backgrounds flock to the site to utilize this fresh approach to learning.

In THE ONE WORLD SCHOOLHOUSE, Khan presents his radical vision for the future of education, as well as his own remarkable story, for the first time. In these pages, you will discover, among other things:

- How both students and teachers are being bound by a broken top-down model invented in Prussia two centuries ago
- Why technology will make classrooms more human and teachers more important
- How and why we can afford to pay educators the same as other professionals
- How we can bring creativity and true human interactivity back to learning
- Why we should be very optimistic about the future of learning.

Parents and politicians routinely bemoan the state of our education system. Statistics suggest we've fallen behind the rest of the world in literacy, math, and sciences. With a shrewd reading of history, Khan explains how this crisis presented itself, and why a return to "mastery learning," abandoned in the twentieth century and ingeniously revived by tools like the Khan Academy, could offer the best opportunity to level the playing field, and to give all of our children a world-class education now.

More than just a solution, THE ONE WORLD SCHOOLHOUSE serves as a call for free, universal, global education, and an explanation of how Khan's simple yet revolutionary thinking can help achieve this inspiring goal.

**The Shallows: What the Internet is Doing to Our Brains (2011)** 280 pgs
Nicholas G. Carr (http://en.wikipedia.org/wiki/Nicholas_G._Carr)
**Summary:**

Finalist for the 2011 Pulitzer Prize in General Nonfiction: "Nicholas Carr has written a *Silent Spring* for the literary mind."—Michael Agger, *Slate*

"Is Google making us stupid?" When Nicholas Carr posed that question, in a celebrated *Atlantic Monthly* cover story, he tapped into a well of anxiety about how the Internet is changing us. He also crystallized one of the most important debates of our time: As we enjoy the Net's bounties, are we sacrificing our ability to read and think deeply?

Now, Carr expands his argument into the most compelling exploration of the Internet's intellectual and cultural consequences yet published. As he describes how human thought has been shaped through the centuries by "tools of the mind"—from the alphabet to maps, to the printing press, the clock, and the computer—Carr interweaves a fascinating account of recent discoveries in neuroscience by such pioneers as Michael Merzenich and Eric Kandel. Our brains, the historical and scientific evidence reveals, change in response to our experiences. The technologies we use to find, store, and share information can literally reroute our neural pathways.

Building on the insights of thinkers from Plato to McLuhan, Carr makes a convincing case that every information technology carries an intellectual ethic—a set of assumptions about the nature of knowledge and intelligence. He explains how the printed book served to focus our attention, promoting deep and creative thought. In stark contrast, the Internet encourages the rapid, distracted sampling of small bits of information from many sources. Its ethic is that of the industrialist, an ethic of speed and efficiency, of optimized production and consumption—and now the Net is remaking us in its own image. We are becoming ever more adept at scanning and skimming, but what we are losing is our capacity for concentration, contemplation, and reflection.

Part intellectual history, part popular science, and part cultural criticism, *The Shallows* sparkles with memorable vignettes—Friedrich Nietzsche wrestling with a typewriter, Sigmund Freud dissecting the brains of sea creatures, Nathaniel Hawthorne contemplating the thunderous approach of a steam locomotive—even as it plumbs profound questions about the state of our modern psyche. This is a book that will forever alter the way we think about media and our minds.