PART III: MODERN AMERICA

The real problem is not whether machines think but whether men do.

– B.F. Skinner[1]

Pages 183-184 are not available in this excerpt.

CORPORATIONS AND GOVERNMENT

The changing balance of power between the public and the top technology and digital media corporations puts the public at serious risk, but the changing balance of power between government and these corporations is equally significant because government and corporations are different in many critical ways.

First, government has checks and balances that no corporations have to the same extent. Market forces are *not* equal to the checks and balances of American government: market forces incentivize both legitimate innovation *and* illegitimate competition. Checks and balances are essential because, if governing bodies fail, people can lose their jobs, their homes, their liberties, and even their lives.

Second, government is far more stable than corporations—it has to be stable due to its immense responsibility. Other nations replace their constitutions every 19 years on average, but the United States Constitution has remained intact since 1787, longer than any constitution ever written[2], not only because it was the first but also because it has stability that other documents have lacked. Sanford Levinson of the University of Texas[3] has said that, of all the world's charters, the United States Constitution is the most difficult to amend: a mere 27 amendments have been ratified since 1787, ten of which came with the Bill of Rights in 1791.[4] Perhaps for government, stability comes at the expense of progress; for corporations, progress comes at the expense of stability.

Third, the public elects government, while individuals build corporations for economic gain. While many corporations have voting systems to some extent, they are fundamentally different

in structure than government. In theory, corporations might have balances of power between managers, boards of directors, and shareholders. In reality, many corporations have boards of directors composed of managers, retired managers, and even family members of managers.[5] Corporations can thus be controlled by an unaccountable few rather than an accountable many.

Because of these essential differences between government and corporations, the changing balance of power between the two sides is of paramount significance: it is a shift in power from government to corporations, from stability to instability, from the generally elected to the individually built, from accountability to the unaccountability, and from democracy to hierarchy.

There is yet a more sinister possibility. As government and corporations struggle for power, as government loses and corporations gain, they grow ever closer and ever more the same. As the President's Council of Advisors on Science and Technology (PCAST) noted in its report to President Obama mentioned earlier: "big data is to some extent a leveler of the differences between government and companies. Both governments and companies have potential access to the same sources of data and the same analytic tools."[6] They also share many of the same goals, whether collecting vast pools of data, analyzing data efficiently, understanding human behavior, or predicting future behavior.

The top technology and digital media corporations depend heavily on the leniency of government big data regulations. Significant leniency currently exists, perhaps in part because the government believes that lesser regulation has helped cultivate the innovation that has propelled America forward during the past several decades.[7] On a deeper level, the United States government generally treats digital privacy as a commodity rather than a fundamental right and relies on sectoral, case-by-case ap-

proaches to privacy harms.[8],* In turn, government depends on corporations: it is enabled by interaction with the private sector in ways that would otherwise be impossible. As PCAST notes, "Current rules may allow government to purchase or otherwise obtain data from the private sector that, in some cases, it could not legally collect itself, or to outsource to the private sector analyses it could not itself legally perform."[11]

PCAST's comments are knowledgeable and seem prescient given the many examples of government utilizing the private sector even without avoiding legal limitations. Two significant examples involve Amazon, one of the largest and most influential technology and digital media corporations in America.† Amazon developed a system for the Securities and Exchange Commission that supplies the bandwidth for its collection of over one billion trade records, a database that grows by more than a terabyte every day. In the summer of 2014, Amazon supplied the CIA with a $600 million computing cloud‡ that all 17 agencies of the government's intelligence network now use.[15] The comments of an unnamed former intelligence officer are telling:

---

* In contrast, the European Union considers privacy a fundamental right and generally regulates big data far more stringently.[9] For example, the EU held in a 2014 ruling that Google and other search engines need to uphold "the right to be forgotten". If European citizens file requests that meet certain requirements, companies must delete data that are "inaccurate, inadequate, irrelevant, or excessive". The ruling has placed an enormous burden on search engines: within only a few days following the ruling, Google received some 50,000 requests to delete data.[10]

† Amazon barely missed my list of focus corporations. Jeff Bezos—Amazon's Founder, President, CEO, and Chairman of the Board[12]—is the 14th wealthiest person in America with total wealth of $28.8 billion.[13]

‡ The government commissioned the computing cloud and also included IBM, Microsoft, AT&T, and undisclosed others in the bidding process.[14]

What we were really looking at was time to mission and innova-
tion. The goal was, "Can we act like a large enterprise in the
corporate world and buy the thing that we don't have; can we
catch up to the commercial cycle? Anybody can build a data cen-
ter, but could we purchase something more?" We decided we
needed to buy innovation.[16]

Government does not only buy innovation and data from main-
stream sources. As discussed in the first part of this book, it pur-
chases personal information from almost entirely unregulated
data brokers, who have enormous databases and operate with
little to no transparency.

It is almost as if PCAST predicted these events, which oc-
curred several months after the group's report, but PCAST's
comments are more honest than clairvoyant. The group *itself* is
an example of the seeming convergence of government and the
private sector: Eric Schmidt (Executive Chairman of Google) and
Craig Mundie (senior advisor to the CEO of Microsoft) are
members of the group and coauthored PCAST's big data report
to the president.[17] It should perhaps be concerning that govern-
ment is using commercial products for intelligence purposes and
that leaders of the top big data corporations are among its closest
advisors. There are glaring conflicts of interest, and the public
has no stake in the game. What is especially troubling is that,
with respect to big data, cooperation between corporations and
government can benefit both sides tremendously, and so it seems
highly likely to continue.

ADVERTISING

Modern advertising is an especially illustrative application of big data. Advertising is an art of persuasion or, said differently, an art of manipulation. Advertisers aim to understand consumers as deeply as possible and then affect their behavior. Since the advent of big data, advertising has become especially pervasive and lucrative, and now it encompasses all three kinds of power I have discussed—economic, political, and social. Advertising underlies the dramatic economic success of the top technology and digital media corporations and thus their economic power. It also plays a critical role in politics. From the election cost data in the political power section of this book, it should be clear that modern American elections are astonishingly expensive—advertising costs likely constitute a huge portion of the billions of dollars spent every cycle. With massive marketing campaigns, candidates and political organizations can attract voters and potential donors. Thus, as advertisers, the top technology and digital media corporations have significant political power. Advertising's role in the social power of these corporations should be self-evident: it is the very practice of influencing people.

Advertising has far more than surface-level effects. Advances in advertising have largely stemmed from new technologies, and new technologies do not only change the ways in which we interact with information—they fundamentally alter our neural pathways.[18] Online advertising, the bedrock of corporations like Google and Facebook, is critically distinct from older forms of advertising, both because it depends on far more information and because it is interactive. We are powerfully affected by the positive reinforcement of clicking on Internet material. As Nicholas Carr (author of *The Shallows*) describes, the Internet "turns us

into lab rats constantly pressing levers to get tiny pellets of social or intellectual nourishment."[19] Lab rats we surely are: "Experiments are run on every user at some point", says a former Facebook data scientist.[20]

The Internet is easily among the most important examples of big data, and it is a technology of distraction. It both fragments our attention and changes our neural networks. Gary Small of the University of California, Los Angeles scanned the brains of experienced Internet users and novices and found significantly different neural activity for the two types of people. He then had the novices use the Internet for an hour each day for five days and subsequently repeated the scans. He found that, after only those *five hours* of using the Internet, the novices exhibited brain activity very similar to that of the experienced Internet users.[21] What is especially shocking is that the Internet as a whole is to some extent a *benign* example because it is a neutral platform for sharing information. If the Internet in general so dramatically alters our neural pathways, to what extent does online advertising, whose very purpose is to influence us?

Corporations like Google, Facebook, Apple, and Microsoft, and by extension the top technology and digital media corporations, depend enormously on effective advertising. They are quite literally in the business of manipulating our behavior, and they are among the best in the world at doing exactly that.

POWERFUL PEOPLE

The people who control the top technology and digital media corporations are both extremely powerful and exceptionally intelligent. Considering the list of people from this book's section

on economic power alone is astonishing: Bill Gates[22], Mark Zuckerberg[23], Steve Ballmer[24], and Dustin Moskovitz[25] attended Harvard University; Larry Page[26], Sergey Brin[27], and Laurene Powell Jobs[28] attended Stanford University; and Eric Schmidt[29] attended Princeton University. These people have impressive pedigrees and have literally shaped the modern world, but the people just beginning in big data are equally intelligent. Harvard's Math 55, which the university calls "probably the most difficult undergraduate math class in the country"[30], is a recruiting ground for the NSA[31]. Stanford University, which last year had the lowest college acceptance rate in the country of 5.07 percent[32], is a recruiting ground for Silicon Valley. The best and the brightest mathematicians, cryptographers, computer programmers, entrepreneurs, and so on are leading the big data revolution, and it is a revolution that has only just begun.

First, assume the best-case scenario. Assume that all of these people are altruistic, model individuals and that they all intend only to improve the world and global society. Even if they have only the best of intentions and the noblest of goals, they are human, make human mistakes, and have human faults. Even absent any corruption, mistakes are not always trivial, and history teaches us that corruption is far from uncommon: needless to say, "absolute power corrupts absolutely."[33] Even if these people could somehow avoid all human vice, they are still mortal. Eventually, other people will replace them, and who can say that the people who do will have admirable moral fiber?

The rhetoric of big data gurus is riddled with contradiction. Google says the Internet works as a democracy[34] while it builds fortresses of data and power. Julian Assange preaches freedom of information but requires his WikiLeaks staff to sign a confidentiality agreement that prohibits them from sharing WikiLeaks ma-

terials (at the threat of a nearly $20 million fine).[35],§ Ideology balks in the face of chaotic reality. The same year they founded Google, Larry Page and Sergey Brin wrote in a scholarly paper, "We expect that advertising-funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."[37]

What if the people who control the top technology and digital media corporations have less than the best of intentions? What if their successors have aims other than making the world a better place? What if these corporations crumble, as all companies are apt to do, and their data are left uncontrolled? The potential dangers of so few people having so much information and so much power are obvious without any hint of conspiracy theory. Everything I have described and all of the speculative questions I have raised are rooted in facts. However, much is still unknown—I will leave extrapolations to you and your imagination. Suffice it to say: *what is* is highly concerning, but *what might be* is terrifying.

TECHNOLOGY AND TERRORISM

Nearly every significant technological advance has potential for both good and bad—such is the nature of great power in general. With steel, we create durable plows but also build dangerous weapons. With antibiotics, we kill dangerous bacteria but also foster drug-resistant "superbugs". With nuclear energy, we operate efficient power plants but also build weapons of mass destruction. Big data is analogous, but I contend that it is vastly more powerful than any other technology in history. Its potential for

---

§ Naturally, the agreement was leaked anonymously.[36]

good is far greater than the benefits of any nuclear reactor, and its potential harms far exceed the destruction of any nuclear weapon.

Consider big data terrorism. We so often worry about physical threats, but I believe the greatest threat is information. What if terrorists had no physical weapons of any kind but knew everything about you—where you live, what car you drive, your phone number, the locations of your family members? Comparing big data and nuclear energy is for more than semantics. Even nuclear energy put to positive use in reactors becomes a target for attack and a potential cause of mass destruction. Data centers are targets as well. When companies and government collect vast amounts of our personal data, they concentrate information geographically and in common formats. Bombing a data center, disrupting the electrical grid, or compromising essential components of digital storage systems could both eliminate vast amounts of information and destroy critical infrastructure of the modern economy.

These physical threats are not the most troubling, however. Just as nuclear reactors are targets for bombing, data centers are targets for hacking. In the past several years, cyberthreats have increased in frequency, scale, sophistication, and impact.[38] Renee James, President of Intel, has said that more than half of the world's computers are sold without security like basic firewalls.[39] 30.03 percent of computers in the United States are infected with some form of malware.[40] Data breaches have increased fivefold since 2009.[41] In 2013, over 13 million Americans were victims of identity theft[42]; in 2014, over 100 million online accounts were compromised in the United States alone[43]. As Assistant to the President for Homeland Security and Counterterrorism Lisa Monaco[44] said in February 2015, "No one connected to the Internet is immune."[45] Hacking poses serious dangers. Groups like

WikiLeaks and Anonymous** proclaim noble goals, but their vigilante justice can accurately be called nonviolent terrorism††. What if violent terrorists had the same capabilities?

The War on Terror has probably been a terribly misguided effort in many ways. The United States has used vast sums of money and resources to fight a small number of people with relatively primitive weapons, all the while fostering public fear for terrorist attacks. If al-Qaeda undermined American society, it did so not so much by destroying the World Trade Center but rather by inciting aggressive reactions from the United States government and inspiring fear in the American public. However, the War on Terror has been misguided in much less obvious ways as well. It directed public focus away from digital privacy and toward physical terrorist threats. It also ended government scrutiny of big data and began the era of modern government surveillance. Congress considered over one dozen bills dealing with online privacy in February 2001, but it abandoned every one of them after the 9/11 attacks seven months later and, in-

---

** Anonymous is not so much a group as a dynamic subculture of "hacktivists" who take justice into their own hands. As one of many examples, when the Church of Scientology requested Gawker Media to remove an online, copyrighted video of Tom Cruise supporting Scientology, Anonymous saw the request as attempted censorship and decided to act against the church. One Anon (as each hacktivist calls him or herself) posted a YouTube video of storm clouds with a computerized voice-over that said, "We shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form. You have nowhere to hide." Anonymous then manipulated Google's search algorithms such that the church's website was at the top of the list of results for "dangerous cult". They also sent a huge number of entirely black faxes to the church's headquarters to drain their machines of ink and marched past Scientology churches in over one hundred cities around the globe. Anonymous has a slogan worthy of any disturbing thriller: "We are Legion. We do not forgive. We do not forget. Expect us."[46]

†† "Terrorism" is such a loaded word, especially in America. Strictly, however, terrorism is "the systematic use of terror especially as a means of coercion".[47] The actions of WikiLeaks and Anonymous certainly fit this definition.

stead, passed the now infamous USA PATRIOT Act.[48] In the course of The War on Terror, the United States government has collected huge amounts of personal information and concentrated it in data centers, effectively peppering the country with targets for physical and cyber terrorist attacks, which could be far more dangerous than any of the terrorist threats The War on Terror is meant to stop!

We now know that much of the government's information comes directly from the private sector. This is probably in large part why the government has not further regulated the top technology and digital media corporations. If it regulated the private sector more stringently, it would lose huge amounts of personal data. As a dangerous side effect of this conflict of interest, the government has allowed largely unregulated corporations to concentrate information in data centers and *further* cover the country with targets for terrorist attacks. There may now be far more and far more potent threats than before The War on Terror began.

ALGORITHMS AND MACHINES

All of the dangers I have mentioned thus far involve people, but the most dangerous threats may be inhuman. More and more, we trust automated, algorithmic systems to accomplish tasks that we cannot or would rather avoid, regardless of whether we can comprehend those systems' internal operations. Even decades ago, at the outset of the Internet age, innovative traders used computer systems to make millions of microtrades every instant. They made steady profits, but the reasoning behind the trades was veiled behind the mechanical rapidity and exactness of the

computers and their algorithms. Modern systems are far more advanced, and we must remember that they are *truly* exact, where exactness may involve inaccuracy or bias. A report to President Obama describes the dangers of algorithmic results: "The final computer-generated product or decision—used for everything from predicting behavior to denying opportunity— can mask prejudices while maintaining a patina of scientific ob-jectivity."[49] Humans do not need to know *why* or *how* an auto-mated system works, only *that* it does. Even *that* a system works means only that it performs as expected over a series of trials: there is no such thing as "proof", and errors can persist even af-ter rigorous testing. Computers and algorithms are grounded in data, but data alone are resources absent any meaning: infor-mation is not knowledge, knowledge is not understanding, and understanding is not wisdom.

Inaccuracy poses obvious problems, but accuracy might in-volve issues as well. What if algorithms could calculate your *actual* propensity for criminal activity? Do we want a world in which automated systems know more about us than we know about ourselves? As Terence Craig (co-author of *Privacy and Big Data* with Mary E. Ludloff) has noted, "Privacy erosion is a subset of secrecy erosion."[50] Secrecy is becoming increasingly difficult to maintain. Our world could rapidly become one of relentless quantification and perhaps brutal truth.

Younger generations are most at risk. Adults today are likely somewhat wary about big data and its potential complications, but young adults are simultaneously less aware of the dangers of big data and affected by them to greater extents. Those born to-day may be completely oblivious to these dangers and will never

know a world without big data.‡ Our society churns forward, and we catalogue our lives to greater and greater extents, perhaps forgetting that computers do not forget. Job applicants are subject to algorithmic evaluations and employees can be fired for Facebook posts[51], but adulthood is hardly the pressing issue: in childhood, especially, forgetting may be crucial. What if every adolescent's mistakes were memorialized in social media archives that are, like all online data, "for all practical purposes, immortal"[52]? How can a child move past his or her mistakes when they may be forever accessible to anyone with sufficient tools? Another concern is that childhood could become an exercise in big data optimization. Already, the intensity of college admissions drives many students to spend their time and energy trying to satisfy the black box algorithms that determine their acceptance or dismissal.

ARTIFICIAL INTELLIGENCE

For now, computers and algorithms still result from human design, but the devices of the future may not. Artificial intelligence (AI) is still relatively primitive and based largely in machine learning, which is the technology behind many modern, "smart" technologies. Machine learning can perhaps be considered "brute force" AI. Google Translate, for example, uses a huge number of language samples to optimize its translation tools using machine-learning techniques. This optimization, however, involves little more than massive computation, and some believe that this kind of "intelligence" is only a crude first step: Douglas

---

‡ I vividly remember seeing a small child swiping at a magazine page, apparently confusing it for the iPad his mother owned.

R. Hofstadter, author of the Pulitzer Prize winning *Gödel, Escher, Bach: An Eternal Golden Braid*, believes that true AI will effectively emulate and then surpass in capability the neural networks of human brains.[53] Future AI could be significantly more efficient and more intelligent than existing machine learning based techniques, which raises difficult technical and ethical questions. Among them: if existing "intelligence" is already somewhat of a black box, how opaque might true AI be?

There is undoubtedly an inexorable march toward AI, and many prominent figures—Bill Gates, Stephen Hawking, and Elon Musk among them—have warned of the dangers of truly intelligent technology[54]. Some people maintain that AI is science fiction fantasy and that no technology could emulate the supposed indiscernible element of humanity. However, if history is any guide, mysticism inevitably yields to science, and the dominion of the soul grows smaller with passing time. The human brain may be nothing more (and nothing less!) than a biological computer, and the breakneck speed of technological advance may soon crack its code.

What if we could outsource more than just information, but knowledge, understanding, and wisdom to machines? What if machines could surpass our mental abilities and develop knowledge, understanding, and wisdom far beyond our own? As I noted in the introduction to this book, we can have great control over our future if we recognize that, for now, a huge portion of the data in today's world depends fundamentally on us. Future AI, however, could change that paradigm and eliminate our chance to regain control. Furthermore, if AI erodes our humanity, it will do so from the bottom to the top, from the powerless to the powerful, from the public to the people who control the top technology and digital media corporations—perhaps the same people who will create future AI.

Pages 199-207 are not available in this excerpt.

THE PERFECT STORM

My earlier digression about Watergate was not without purpose, and it was not merely to show degradation of trust in American government. I truly fear that it may take a Watergate-like event to create big data awareness and inspire public pressure for reform. If this concern seems unfounded or premature, consider the surprising number of parallels between Watergate and the current situation. Just as Nixon was extremely popular before the election of 1972, the top technology and digital media corporations are extremely popular today. Just as campaign finance regulations before Watergate had serious shortcomings (as evidenced by Nixon's illegal actions and the FECA amendments that followed the scandal), current campaign finance regulations allow for unlimited corporate donations with no transparency and therefore no accountability. Just as Nixon's burglars wiretapped the Watergate complex and stole confidential documents, modern government and corporate entities are engaging in widespread surveillance and collecting large amounts of personal data. Just as Nixon refused to comply with investigators, data brokers have denied repeated requests for information from a Senate investigatory committee. However, despite all of these troubling parallels, there is perhaps a glimmer of hope: just as the White House tapes (Nixon's self-surveillance) finally ended Watergate, big data may help solve the many dangers it poses.

There is a perfect storm brewing. Overpopulation is racking the globe just as automation and robotics are eliminating jobs. The inexorable drive toward artificial intelligence could further exacerbate unemployment and reduce the transparency of already opaque algorithms. Potent cyberthreats are greatly endangering individual consumers and entire economies alike, and we

lack sufficient cybersecurity. Power has shifted to corporations and to startup companies that have none of the stability of governing bodies and operate on speculative and sometimes highly risky premises. America has some of the highest wealth and income inequalities of anywhere in the world. If the widespread speculation and economic inequality preceding the Great Depression provide any indication, there could be another dramatic financial crash on the horizon. Government big data regulations, which may be necessary to solve big data's problems, are inhibited by the powerful incentives for both corporations and government to collect as much data as possible and could be further inhibited by a conservative shift in American government. There is an extreme concentration of economic, political, and social power in the hands of the people who control the top technology and digital media corporations, and they have the financial means, popularity, public presences, and vast databases to maintain and increase their power.

None of these factors necessarily involve any kind of conspiracy or corruption: a dystopian future could result merely from a lack of awareness and the sometimes shortsighted and reckless idealism that defines modern big data innovation. However, if conspiracy or corruption is a factor as well, the future could be distressingly dark. We, the American public, stand largely oblivious beneath the coming storm. I profoundly hope that it will not take Datagate to make us aware of big data's dangers. I cannot help but wonder—if Datagate happens, will there be any White House tapes?

★ ★ ★ ★ ★

Relevant endnotes are included on the following pages.

Web. 17 Jan. 2015. <http://www.nytimes.com/2010/11/29/world/29cab les.html?pagewanted=all+%28>.

196 Timm, Trevor. "Cablegate One Year Later: How WikiLeaks Has Influenced Foreign Policy, Journalism, and the First Amendment." *Electronic Frontier Foundation*. Electronic Frontier Foundation, 28 Nov. 2011. Web. 23 Feb. 2015. <https://www.eff.org/deeplinks/2011/11/cablegate-one-year-later-how-wikileaks-has-influenced-foreign-policy-journalism>.

197 "Kissinger Cables: Wikileaks Publishes 1.7m US Diplomatic Documents from 1970s." *The Telegraph*. Ed. Bonnie Malkin. Telegraph Media Group Limited, 8 Apr. 2013. Web. 17 Jan. 2015. <http://www.telegraph.co.uk/ news/wikileaks-files/9977979/Kissinger-Cables-Wikileaks-publishes-1.7m-US-diplomatic-documents-from-1970s.html>.

SECTION 5: INFLUENCE

1 "The World's Most Powerful Brands." *Ranking the Brands*. SyncForce, n.d. Web. 12 Jan. 2015. <http://www.rankingthebrands.com/The-Brand-Rank ings.aspx?rankingID=279&nav=category>.

2 *Ibid.*

3 *Ibid.*

4 "Google Named Most Influential Brand in the United States." *Ipsos*. Ipsos, 14 Mar. 2013. Web. 12 Jan. 2015. <http://www.ipsos-na.com/news-polls/ pressrelease.aspx?id=6034>.

5 *Ibid.*

6 "Brand Dependence Index Debuts." *UTA Brand Studio*. United Talent Agency, 12 Feb. 2014. Web. 12 Jan. 2015. <http://utabrandstudio.com/ brand-dependence-index-debuts/>.

7 *Ibid.*

8 "Brand Desire 2013." *Issuu*. Issuu, 2013. Web. 12 Jan. 2015. <http://issuu. com/clear-ideas/docs/branddesire/50#>.

PART III: MODERN AMERICA

1 "B.F. Skinner Quotes." *Goodreads*. Goodreads, n.d. Web. 14 Feb. 2015. <http://www.goodreads.com/quotes/266200-the-real-question-is-not-whe ther-machines-think-but-whether>.

2 Liptak, Adam. "'We the People' Loses Appeal With People Around the World." *The New York Times*. The New York Times, 06 Feb. 2012. Web. 11 Feb. 2015. <http://www.nytimes.com/2012/02/07/us/we-the-people-loses-appeal-with-people-around-the-world.html?_r=0>.

3 "Sanford V. Levinson." *School of Law: The University of Texas at Austin*. The University of Texas School of Law, n.d. Web. 11 Feb. 2015. <http://www.utexas.edu/law/faculty/svl55/>.

4 *See supra* note 2.

5 "The Basics Of Corporate Structure." *Investopedia*. Investopedia, n.d. Web. 9 Feb. 2015. <http://www.investopedia.com/articles/basics/03/022803.asp>.

6 Holdren, James P., Eric S. Lander, William Press, Maxine Savitz, Rosina Bierbaum, S. James Gates, Jr., Christine Cassel, Mark Gorenberg, Christopher Chyba, Susan L. Graham, Shirley Ann Jackson, Craig Mundie, Richard C. Levin, Ed Penhoet, Michael McQuade, Barbara Schaal, Chad Mirkin, Eric Schmidt, Mario Molina, and Daniel Schrag. "Big Data and Privacy: A Technological Perspective." *President's Council of Advisors on Science and Technology: Report to the President* (2014): n. pag. 1 May 2014. Web. 29 Jun. 2014. <http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>.

7 Podesta, John, Penny Pritzker, Ernest J. Moniz, John Holdren, and Jeffrey Zients. "Big Data: Seizing Opportunities, Preserving Values." *Executive Office of the President Report* (2014): n. pag. 1 May 2014. Web. 11 Sept. 2014. <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

8 Craig, Terence, and Mary E. Ludloff. *Privacy and Big Data*. Sebastopol, CA: O'Reilly, 2011. Print.

9 *Ibid.*

10 Wohlsen, Marcus. "For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco." *Wired*. Condé Nast Digital, 3 July 2014. Web. 11 Feb. 2015. <http://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/>.

11 *See supra* note 6.

12 "Officers & Directors." *Amazon*. Amazon, n.d. Web. 10 Sept. 2014. <http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-govmanage>.

13 "Forbes 400." *Forbes*. Forbes Magazine, 2014. Web. 1 Jan. 2015. <http://www.forbes.com/forbes-400/list/>.

14 Konkel, Frank. "How the CIA Partnered With Amazon and Changed Intelligence." *Defense One*. National Journal Group, Inc., 11 July 2014. Web. 11 July 2014. <http://www.defenseone.com/technology/2014/07/how-cia-partnered-amazon-and-changed-intelligence/88555/>.

15 *Ibid.*

16   *Ibid.*
17   *See supra* note 6.
18   Carr, Nicholas G. *The Shallows: What the Internet Is Doing to Our Brains*. New York: W.W. Norton, 2010. Print.
19   *Ibid.*
20   Hill, Kashmir. "Ex-Facebook Data Scientist: Every Facebook User Is Part Of An Experiment At Some Point." *Forbes*. Forbes Magazine, 7 July 2014. Web. 10 Feb. 2015. <http://www.forbes.com/sites/kashmirhill/2014/07/07/ex-facebook-data-scientist-every-facebook-user-is-part-of-an-experiment-at-some-point/>.
21   *See supra* note 18.
22   "Bill Gates Biography." *Bio.com*. A&E Networks Television, n.d. Web. 27 Jan. 2015. <http://www.biography.com/people/bill-gates-9307520#synopsis>.
23   "Mark Zuckerberg Biography." *Bio.com*. A&E Networks Television, n.d. Web. 27 Jan. 2015. <http://www.biography.com/people/mark-zuckerberg-507402>.
24   "Steve Ballmer." *Forbes*. Forbes Magazine, n.d. Web. 27 Jan. 2015. <http://www.forbes.com/profile/steve-ballmer/>.
25   "Dustin Moskovitz." *Forbes*. Forbes Magazine, n.d. Web. 27 Jan. 2015. <http://www.forbes.com/profile/dustin-moskovitz/>.
26   "Larry Page Biography." *Bio.com*. A&E Networks Television, n.d. Web. 27 Jan. 2015. <http://www.biography.com/people/larry-page-12103347>.
27   "Sergey Brin Biography." *Bio.com*. A&E Networks Television, n.d. Web. 27 Jan. 2015. <http://www.biography.com/people/sergey-brin-1213333>.
28   "Laurene Powell Jobs & Family." *Forbes*. Forbes Magazine, n.d. Web. 27 Jan. 2015. <http://www.forbes.com/profile/laurene-powell-jobs/>.
29   "Eric Schmidt." *Forbes*. Forbes Magazine, n.d. Web. 27 Jan. 2015. <http://www.forbes.com/profile/eric-schmidt/>.
30   "Harvard Mathematics Department 21, 23, 25, or 55?" *Department of Mathematics*. The President and Fellows of Harvard College, n.d. Web. 17 Feb. 2015. <http://www.math.harvard.edu/pamphlets/freshmenguide.html>.
31   Rudder, Christian. *Dataclysm: Who We Are (When We Think No One's Looking)*. New York: Crown, 2014. Print.
32   Zivkovic, Alex. "Class of 2018 Admit Rates Lowest in University History." *The Stanford Daily*. The Stanford Daily, 28 Mar. 2014. Web. 27 Jan. 2015.
33   Martin, Gary. "The Meaning and Origin of the Expression: Power Corrupts; Absolute Power Corrupts Absolutely." *The Phrase Finder*. Gary Martin, n.d. Web. 11 Feb. 2015. <http://www.phrases.org.uk/meanings/absolute-power-corrupts-absolutely.html>.

34 "Ten Things We Know to Be True." *Google*. Google, n.d. Web. 11 Feb. 2015. <http://www.google.com/about/company/philosophy/>.

35 Poulsen, Kevin. "WikiLeaks Threatens Its Own Leakers With $20 Million Penalty." *Wired*. Condé Nast Digital, 11 May 2011. Web. 11 Feb. 2015. <http://www.wired.com/2011/05/nda-wikileaks/>.

36 *Ibid.*

37 *See supra* note 18.

38 Monaco, Lisa. "Introductory Remarks." White House Summit on Cybersecurity and Consumer Protection. Stanford University, Memorial Auditorium, Stanford, CA. 13 Feb. 2015. Speech.

39 James, Renee. "Second Plenary Panel: Improving Cybersecurity Practices at Consumer Oriented Businesses and Organizations." White House Summit on Cybersecurity and Consumer Protection. Stanford University, Memorial Auditorium, Stanford, CA. 13 Feb. 2015. Speech.

40 Samson, Ted. "Malware Infects 30 Percent of Computers in U.S." *InfoWorld*. InfoWorld, Inc., 8 Aug. 2012. Web. 17 Feb. 2015. <http://www.infoworld.com/article/2618043/cyber-crime/malware-infects-30-percent-of-computers-in-u-s-.html>.

41 *See supra* note 38.

42 Cook, Tim. "Remarks." White House Summit on Cybersecurity and Consumer Protection. Stanford University, Memorial Auditorium, Stanford, CA. 13 Feb. 2015. Speech.

43 Zients, Jeff. "Introductory Remarks." White House Summit on Cybersecurity and Consumer Protection. Stanford University, Memorial Auditorium, Stanford, CA. 13 Feb. 2015. Speech.

44 "Remarks by Assistant to the President for Homeland Security and Counterterrorism Lisa O. Monaco." *The White House*. The White House, 16 Apr. 2014. Web. 17 Feb. 2015. <http://www.whitehouse.gov/the-press-office/2014/04/16/remarks-assistant-president-homeland-security-and-counterterrorism-lisa->.

45 *See supra* note 40.

46 Kushner, David. "The Masked Avengers." *The New Yorker*. Condé Nast Digital, 8 Sept. 2014. Web. 11 Feb. 2015. <http://www.newyorker.com/magazine/2014/09/08/masked-avengers>.

47 "Terrorism." *Merriam-Webster*. Merriam-Webster, n.d. Web. 11 Feb. 2015. <http://www.merriam-webster.com/dictionary/terrorist>.

48 *Terms and Conditions May Apply*. Dir. Cullen Hoback. Perf. Max Schrems, Moby, Mark Zuckerberg. Hyrax Films, Topiary Productions, 2013. Netflix Streaming.

49 *See supra* note 7.

50 *See supra* note 8.

51 Bean, Daniel. "11 Brutal Reminders That You Can and Will Get Fired for What You Post on Facebook." *Yahoo*. Yahoo, 6 May 2014. Web. 27 Jan. 2015. <https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html>.

52 *See supra* note 8.

53 Somers, James. "The Man Who Would Teach Machines to Think." *The Atlantic*. Atlantic Media Company, 23 Oct. 2013. Web. 11 Feb. 2015. <http://www.theatlantic.com/magazine/archive/2013/11/the-man-who-would-teach-machines-to-think/309529/>.

54 Kohli, Sonali. "Bill Gates Joins Elon Musk and Stephen Hawking in Saying Artificial Intelligence Is Scary." *Quartz*. Quartz, 30 Jan. 2015. Web. 11 Feb. 2015. <http://qz.com/335768/bill-gates-joins-elon-musk-and-stephen-hawking-in-saying-artificial-intelligence-is-scary/>.

55 Constantin, Lucian. "Blackphone's Super-secure Communications App Had Serious Flaw." *PCWorld*. IDG Consumer & SMB, 28 Jan. 2015. Web. 11 Feb. 2015. <http://www.pcworld.com/article/2876772/blackphone-supersecure-communications-app-had-serious-flaw.html>.

56 Leswing, Kif. "Ad Tech Firm Ghostery Releases a Privacy-focused Android Browser." *Gigaom*. Gigaom, Inc., 3 Dec. 2014. Web. 11 Feb. 2015. <https://gigaom.com/2014/12/03/ad-tech-firm-ghostery-releases-a-privacy-focused-android-browser/>.

57 *See supra* note 55.

58 Bilton, Ricardo. "Ghostery: A Web Tracking Blocker That Actually Helps the Ad Industry." *VentureBeat*. VentureBeat, 31 July 2012. Web. 11 Feb. 2015. <http://venturebeat.com/2012/07/31/ghostery-a-web-tracking-blocker-that-actually-helps-the-ad-industry/>.

59 "Frequently Asked Questions." *Ghostery*. Ghostery, Inc., n.d. Web. 11 Feb. 2015. <https://www.ghostery.com/en/faq#q5-general>.

60 Lanier, Jaron. *Who Owns the Future?* London: Penguin (Allen Lane), 2013. Print.

61 Stravinsky, Igor, Arthur Knodel, and Ingolf Dahl. *Poetics of Music: In the Form of Six Lessons*. Cambridge: Harvard UP, 1947. Print.

62 Wohlsen, Marcus. "Larry Page Lays Out His Plan for Your Future." *Wired*. Condé Nast Digital, 19 Mar. 2014. Web. 11 Feb. 2015. <http://www.wired.com/2014/03/larry-page-using-google-build-future-well-living/>.

63 *See supra* note 31.

64 *Ibid.*

65 "Biographies of Current Justices of the Supreme Court." *Supreme Court of the United States*. Supreme Court of the United States, 4 Jan. 2015. Web. 17 Jan. 2015. <http://www.supremecourt.gov/about/biographies.aspx>.

66 "Republicans Seize Control of Senate, Retain House." *The Wall Street Journal*. The Wall Street Journal, 5 Nov. 2014. Web. 17 Jan. 2015. <http://