EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

New Perspectives on (Anti)Social Media

Hal Berghel, University of Nevada, Las Vegas

Much has been written recently about the political problems caused by antisocial media. Here's an account of two very different perspectives on the causes and consequences.

What do we make of the recent spate of criticism of the major social media monopolies like Google, Facebook, WhatsApp, Instagram, Twitter, TikTok, and the like? Or, to put the matter differently, what is their overall social impact on our information society? Are these platforms legitimately improving the social mobility and inclusiveness of society, or are such claims proffered as thin veneers to conceal abusive monopolies that masquerade as servants of the public interest? These are important questions that are insufficiently addressed by the public and politicians, and they are only slightly better addressed by mainstream media. The reasons for this are manifold: the enormous lobbying power of social media companies, interconnected interests of these companies and commercial media, technical barriers to journalists' understanding of the underlying platforms, unwillingness on the part of politicians to openly challenge the business models of powerful tech companies, and, most importantly, the lack of sufficient political support for protecting the privacy of U.S. citizens.

There was no federal protection of personal privacy in the United States from its founding. This was by design—and the current economic and political power base of the country wants it to stay that way. If there was a single factor that ties together identity theft, credit card fraud, computer crimes, online trolling, phish scams, and title fraud on the one hand with partisan political manipulation by gerrymandering, voter disenfranchisement, and vote suppression (by caging, purging, vote nullification, dilution disinformation streams, and so on) on the other, it is the absence of federal privacy protections for citizens. As I've written about these topics before,[1–4] we needn't go into them here. Suffice it to say that business and commercial interests have prevailed upon politicians to consistently support corporate interests (such as the right to make money) over public interests (such as the right to be left alone) in this regard. The Equifax hack and the Cambridge Analytica scandal are two sides of the same coin; they are both consequences of commercial and/or partisan interests profiting from the use of personal information

Digital Object Identifier 10.1109/MC.2019.2958448
Date of current version: 12 March 2020

without the knowledge, permission, and regard of the people involved.

It is a mistake of the first order to attribute the outcomes of these two events (in the case of Equifax, the loss of personally identifiable information of half the adult population in the United States to cybercriminals, and in the case of Cambridge Analytics, microtargeting of Facebook users and "friends" by partisan political operatives) to coincidence. These consequences were not accidents. These were entirely predictable outcomes of socially irresponsible uses of personal data—which are legal in the United States.[5,6] There is a reason why commercial and partisan interests vigorously and uniformly oppose such notions as requiring an opt-in for online services, net neutrality, data collection transparency, and others.

These interests would have us believe that stealth blocking, content filtering, traffic shaping, and protocol discrimination are tools that Internet service providers may use to enhance customer satisfaction with their networks. Taken together, these concepts underscore the fact that citizen consumers are first and foremost products of online platforms and only secondarily customers or users. Further, online platform businesses hold that these human products have no inherent rights that corporate interests are bound to recognize. We are in a new Lochner era where Congress and the courts are comfortable with the seemingly unrestricted corporate use of a citizen's personal information. As with the original Lochner era a century ago, the prevailing political and legal view subsumes corporate rights under the 14th Amendment's due process clause for corporate freedom of contract. This is new millennium neoliberalism at its finest.

This point is made most dramatically by studying the effects of federal financial integrity legislation in the Sarbanes–Oxley Act (SOX). Motivated by the accounting scandals of Enron, WorldCom, and Tyco, Congress passed SOX to hold key executives of corporations personally liable for frauds taking place under their leadership. But only rarely do financial crime convictions result from SOX prosecutions.[7] It seems more likely that such control fraud convictions will result from state faithless servant prosecutions within the few states that have such laws. To illustrate, the first prosecution of a chief executive officer (CEO) under SOX was that of Richard Scrushy, CEO of HealthSouth in 2003, which led to an acquittal despite overwhelming evidence.[8,9] Scrushy's subsequent conviction and imprisonment were for bribery, conspiracy, and mail fraud unrelated to the SOX prosecution.

> There are just some scholarly topics that aren't amenable to YouTube, clickstreams, and 30-min news cycles. Mass manipulation is one of them.

The lack of corporate accountability is well documented when it comes to antisocial media as well as corporate fraud. The latter point has been well documented of late by two authors with very different perspectives: venture capitalist Roger McNamee and political communications researcher and university professor Kathleen Hall Jamieson.[10,11] Although they approach the problem from very different perspectives, their views are surprisingly congruent.

ZUCKING AMERICA

McNamee was an early investor in Facebook, and while his technical understanding of the platform (and computing, for that matter) may not intoxicate the broader computer science and engineering audience, his social commentary seems to be spot on (unusual for a venture capitalist from my experience). I'll pick a few nits to illustrate the deficiencies of his commentary. First, McNamee summarizes Metcalfe's law as describing the geometric growth of the value of a network. Metcalfe described it as quadratic growth. Second, he states that networking began around a single minicomputer, ignoring the significantly earlier mainframe contributions of IBM (remote spooling and communications subsystem/Vnet), Network Systems' HYPERchannel, American Airlines, SABRE reservation system, Control Data's PLATO environment, and other mainframe-centric systems. There are even some whoppers like "with the exception of Digital Equipment, all of the market leaders of the past still exist today." When was the last time you saw computers by Control Data, Univac, General Electric, RCA, Burroughs, Sperry Univac, NCR, and Honeywell advertised? While the first half of the book is sprinkled with dozens of off-putting lapses of the pen, the last half, which focuses on the abuses of social media platforms, offers some useful (if unorthodox) perspectives from a venture capitalist that are worthwhile even to a technical computing audience.

McNamee introduces the topic of social media by reference to the research in computer persuasion by Stanford behavioral scientist B.J. Fogg.[12] This was an exceedingly good narrative strategy for it is impossible to fully understand the success of social media (and the Cambridge Analytica scandal for that matter) without reading Fogg. From a scholarly perspective, Fogg's work falls somewhere within a triangle whose vertices are represented by Edward Bernays, Stanley Milgram, and Ron Popeil. Fogg uses experimental psychology techniques to study how computing technology can be used persuasively. Of course, there is a darker

side to this research highlighted by our vertices: how computing technology can be misused persuasively. One example of that would be what I have called *abuse-forming networks*.[14]

However, beginning the analysis with Fogg was inspired for it lays bare the motivations behind social media platforms as such and in general. To quote McNamee:

> *...computing devices allow programmers to combine psychology and persuasion concepts ... like propaganda with techniques from slot machines, like variable rewards, and tie them to the human social need for approval and validation in ways that few users can resist.*[10]

That is essentially the observation that binds Edward Bernays, Stanley Milgram, and Ron Popeil. They were all masters of the practice of manipulating unsuspecting subjects. This is an underappreciated dimension of our human predicament. There are a lot of people who are interested in getting others to do things that they normally wouldn't be inclined to do—from applying painful electric shocks to innocent victims, to getting women to smoke cigarettes, to talking people into buying Veg-O-Matics and Pocket Fishermen. It's all about manipulation, and Fogg is an important contributor to the scholarship behind social media's manipulation of the unsuspecting.

The payoffs for social media manipulation (toward both social good and bad) are much greater than were available before computer networks (for example, through direct mailing and print advertising). McNamee points out that some of the downsides include encouraging tribalism through preference and filter bubbles, legitimizing extremism, using anonymity to reduce the barriers to antisocial expression, desensitizing people to racist and antisemitic rants, building and propagating conspiracy theories, delegitimizing opposing views by inflammatory disinformation, and so on. McNamee cautions that

> *...if you are a bad actor and you want to manipulate people in a preference bubble, all you have to do is infiltrate the tribe, deploy the appropriate dog whistles, and you are good to go. That is what the Russians did with the U.S. presidential election in 2016 and what many are doing now.*[10]

It is important to add that these techniques are not new to, but were exacerbated by, social media. The most successful tyrants and dictators in history were devotees of such techniques but, until recently, were denied access to the technology platforms that brought the techniques to the current level of maturity and convenience. It should also be emphasized that the dynamics behind such manipulative strategies have been widely discussed in the scholarly literature for decades. Herman and Chomsky's seminal work, *Manufacturing Consent*,[15] and two of Jason Stanley's recent books provide a yeoman's understanding.[16,17] The problem is not that scholars don't understand the practice of mass manipulation but rather that so much of the public chooses to remain willfully ignorant of it. There are just some scholarly topics that aren't amenable to YouTube, clickstreams, and 30-min news cycles. Mass manipulation is one of them.

One of the deficiencies of Fogg's analysis is that it fails to adequately emphasize the influence of cognitive biases on the ascription of credible sources. Tribalists are more likely to perceive information as credible when it accords with their own preconceptions (confirmation bias). Fogg tends to ascribe far too much to end-user gullibility[18] and not nearly enough to the psychological realities of rational deficits such as cognitive dissonance.[19] McNamee reflects on the use of Fogg's tool kit to accomplish such manipulation: "technology companies [devote] some of their best minds to exploiting the weaknesses in human psychology."[10] The only change I might make is to substitute "realities" for "weaknesses."

That caveat notwithstanding, McNamee seems to understand our present predicament quite well. McNamee and I divide mostly on the issue of motive. What McNamee doesn't recognize is that the business practices of Facebook and Google are closer to those of Enron and Theranos than they are to Hewlett-Packard and Microsoft. In my view, McNamee's attribution of honorable motives to social media companies like Facebook is both naïve and misplaced. It is not so much that the executives of these companies are immoral, but amoral. Considerations of truth, justice, fairness, diversity, rights to privacy, and so on do not appear on their compass cards. Facebook's motto was "move fast and break things" and not "proceed cautiously and be mindful of the rights of others."

What McNamee doesn't recognize is that the business practices of Facebook and Google are closer to those of Enron and Theranos than they are to Hewlett-Packard and Microsoft.

It is worthwhile to reflect on the guiding principles of the social media companies by noticing the gap between these principles and the Association for Computing Machinery Code of Ethics and Professional Conduct,

especially the sections on doing no harm, respecting privacy, honoring confidentiality, and treating people fairly.[13] It is important to reemphasize that social media participants are first and foremost products that can be monetized and are only secondarily customers, end users, and citizens. McNamee underscores that the Cambridge Analytica story shows that society must look at social media platforms in terms of the total cost of ownership or, more accurately perhaps, the total cost of abuse.[14] Similar points are to be found in other recent books on antisocial media.[6,20,21]

McNamee's significant contribution to the study of social media in general, and Facebook in particular, comes at the end of the book. The last two chapters consist of policy recommendations that are well thought through and worthy of consideration.

DIGITAL MERCENARIES AND THEIR GASLIT NATIONS

The 2016 polls were right—at least in terms of predicting popular vote. For example, the prediction by Nate Silver's FiveThirtyEight was a 4% popular vote lead for Clinton.[25–27] The final result was a 2.1% popular vote advantage for Clinton, well within a reasonable margin of error.[28] It is well documented that the 2016 election was one of five in the history of the United States (1824, 1876, 1888, 2000, 2016) where the winner of the popular vote failed to be elected. On balance, the 2016 polls accurately predicted what they purported to survey: popular opinion. What they did not do is accurately predict the effects of digital mercenaries and gaslighting and the subsequent effects on the electoral college outcome. For example, they did not see that the electoral vote would be determined by 75,000 votes in only three states—and that these voters would be the objects of sophisticated microtargeting. This is the starting point of Kathleen Hall Jamieson's recent book, *Cyber-War*, which elaborates on the problems that McNamee addresses though through the lens of a social scientist.[11]

Whereas McNamee approached social media abuses from a business point of view, Jamieson sees it from the perspective of political communication. Put simply, McNamee emphasizes the uses of social media to control the political conversation, while Jamieson emphasizes the effects of social media on the body politic. Their positions are remarkably congruent, given their different interests. Taken together, they make a compelling case that the relationship between social media and the political conversation needs to be carefully studied by computing and social scientists.

Based on its partisan involvement in the 2016 U.S. presidential election, Wikileaks might be best viewed among others as an asymmetrical information disintermediator.

In addition, 2016 revealed the potential of social mediators like Wikileaks as a political weapon as well as an information conduit. Based on its partisan involvement in the 2016 U.S. presidential election, Wikileaks might be best viewed among others as an asymmetrical information disintermediator, an information source that receives, filters, and distributes real source data that conform to a particular agenda—in this case a partisan one. Jamieson persuasively argues that the Wikileaks dump of John Podesta's stolen emails shortly after the *Access Hollywood* tape release completely reframed the political narrative two days before the second presidential debate. I know of no reputable scholar or journalist who feels that these two events were coincidental.

This changed the narrative in two ways. First, it directed the attention away from Trump's indiscretions and toward the confidential, internal workings of Hillary Clinton's campaign, warts and all. This provided ammunition for Trump supporters who were in desperate search for a deflection point to distract attention away from the *Access Hollywood* tape release. But more importantly, as Jamieson shows, it targeted Wikileaks as the source of the Podesta leak in the mind of the public when Russians were the actual source.[22] In terms of our new nomenclature, Wikileaks served as an asymmetrical information disintermediator between the Russian hackers who retrieved Podesta's emails and the public. Note that this distinction is critical to the understanding of the event. Had the public and the Trump campaign been informed that Russian agents were the source of the emails, the partisan value of the information would have diminished. The commercial media may be legitimately faulted for failing to emphasize this distinction. This was an example of the harmful effects of short-form journalism. There was no I.F. Stone or George Seldes to carry the burden of investigative reporting to be found anywhere near this issue in real time.

In one sense, McNamee may be looking at social media dystopia proactively, while Jamieson is viewing it reactively. Taken together, they offer a rather complete overview of the digital gaslighting that we've witnessed over the past decade or so. For those of us involved in computing and networking technology and public policy, the questions we must address relate to how this manipulation works, both from the point of view of deployment (such as perception management, social engineering, and microtargeting on hot button issues) as well as the effect of

nurturing sundry forms of tribalism (religious, racial, ethnic, ultranationalist, ideopolitical, antiimmigrant, and so on). To study one of these dimensions without the other will preclude an adequate understanding of the political abuse of antisocial media in a historical context. For example, the public manipulation that preceded genocides (Nazi, Hutu, Janjaweed, and Khmer Rouge, for example) seemed to be tribal-inspired efforts not unlike those in use by today's social media cyber mercenaries.

Jamieson suggests that the 2016 U.S. election disinformation campaigns proved two things:

1. Disinformation is a powerful tool for engaging and energizing tribes.
2. There is minimal political or legal penalty for such aggressive, offensive tactics.

(It may be worthwhile to consider my remarks about SOX in this regard.) Consider that the successful prosecutions resulting from the recent Mueller investigation[23] were for such things as making false statements to the FBI, fraud, witness tampering, campaign finance laws, and lying to Congress—not for using social media campaigns to subvert a presidential election. Now that we have a fuller understanding of what happened in 2016, we should be asking ourselves what are the future hot-button issues that will trigger the tribes and how we may prepare for the continued weaponization of social media because the continued use of social media for disinformation campaigns is a foregone conclusion. Genetically modified organisms, global warming, racism, bigotry, white supremacy, antiimmigration, antiliberal, and sundry other examples of fear mongering will continue to be useful hot-button issues for disinformationalists. To repurpose a phrase from Blaise Pascal, democracy demands a prepared mind.

I'll use the term *lizard brain populism* to refer to a sociopolitical–economic ecosystem that drives social media disinformation. It is important to recognize that the money behind both social media platforms and K-Street lobbyists have the same sources and motives. They are both grounded in public manipulation, and their business models are neither public spirited nor citizen centric. In addition, another concomitant effect of the disinformation (or propaganda) is what Alexi Yurchak calls *hypernormalization*, where the culture becomes so accustomed to the disinformation (also known as *fake news*) that they're willing to accept any alternative as viable no matter how absurd.[24] In Jamieson's terms, "Activated cynicism depresses learning."[29] We might think of hypernormalization as cultural social engineering.

I'll use the term *lizard brain populism* to refer to a sociopolitical–economic ecosystem that drives social media disinformation.

To say that the targets of social media have gullibility in common is too simplistic. To paraphrase P.T. Barnam, there are different tranches of social media "suckers" born every minute. For example, in the case of the Cambridge Analytica scandal, there wasn't much overlap between those who fell for the "this is your digital life" application (app) ruse and the victims of the subsequent microtargeting effort. The former might well be admonished for failure to read the app's (and Facebook's) licensing agreement, but this admonishment wouldn't apply to the victims of the subsequent political microtargeting. Each of these tranches merits separate study. And while the snarky among us might claim that the common theme is the lure of both groups to the shallow reaches of the gene pool, the fact is that each victim group is best viewed as sociologically or psychologically distinct. The digital manipulators and abusers among us understand this quite well. It is the public—and perhaps a smattering of computing professionals—that fails to adequately appreciate such distinctions. It is the responsibility of the informed of any stripe to educate the uninformed to mitigate against future abuses that result from confusion over the myth math of ideas flowing out of the social media platforms.

REFERENCES

1. H. Berghel, "Digital politics 2016," *Computer*, vol. 49, no. 1, pp. 75–79, Jan. 2016. doi: 10.1109/MC.2016.23. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7383164
2. H. Berghel, "Equifax and the latest round of identity theft roulette," *Computer*, vol. 50, no. 12, pp. 72–76, Dec. 2017. doi: 10.1109/MC.2017.4451227. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8220474
3. H. Berghel, "Malice domestic: The Cambridge analytica dystopia," *Computer*, vol. 51, no. 5, pp. 84–89, May 2018. doi: 10.1109/MC.2018.2381135. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8364652
4. H. Berghel, "Disinformatics: The discipline behind grand deceptions," *Computer*, vol. 51, no. 1, pp. 89–93, Jan. 2018. doi: 10.1109/MC.2018.1151023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8268033
5. "How Equifax neglected cybersecurity and suffered a devastating data breach," U.S. Senate Permanent Subcommittee on Investigations, Committee on Homeland Security

and Government Affairs, Washington, D.C., 2018. [Online]. Available: https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf
6. C. Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America*. New York: Random House, 2019.
7. K. Seymour, "Sarbanes–Oxley's lost promise: Why CEOs haven't been prosecuted," *Reuters*, July 27, 2012. [Online]. Available: http://blogs.reuters.com/alison-frankel/2012/07/27/sarbanes-oxleys-lost-promise-why-ceos-havent-been-prosecuted/
8. "Healthsouth founder and former CEO Richard Scrushy charged in $2.7 billion accounting fraud conspiracy," U.S. Department of Justice, Washington, D.C., Nov. 4, 2003. [Online]. Available: https://www.justice.gov/archive/opa/pr/2003/November/03_crm_603.htm
9. K. Crawford, "Ex-HealthSouth CEO Scrushy walks," *CNN Money*, June 28, 2005. [Online]. Available: https://money.cnn.com/2005/06/28/news/newsmakers/scrushy_outcome/index.htm
10. R. McNamee, *Zucked: Waking up to the Facebook Catastrophe*. Baltimore, MD: Penguin, 2019.
11. K. H. Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President*. London: Oxford Univ. Press, 2018.
12. B. J. Fogg, "Persuasive technologies," *Commun. ACM*, vol. 42, no. 5, pp. 26–29, May 1999. doi: 10.1145/301353.301396. [Online]. Available: https://cacm.acm.org/magazines/1999/5
13. Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," New York, 2018. [Online]. Available: https://www.acm.org/code-of-ethics
14. H. Berghel, "Weaponizing Twitter litter: Abuse-forming networks and social media," *Computer*, vol. 51, no. 4, pp. 70–73, Apr. 2018. doi: 10.1109/MC.2018.2141019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8352071
15. E. Herman and N. Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*. New York: Pantheon Books, 2002.
16. S. Jason, *How Propaganda Works*. Princeton, NJ: Princeton Univ. Press, 2016.
17. J. Stanley, *How Fascism Works: The Politics of Us and Them*. New York: Random House, 2018.
18. S. Tseng and B. J. Fogg, "Credibility and computing technology," *Commun. ACM*, vol. 42, no. 5, pp. 39–44, May 1999. doi: 10.1145/301353.301402. [Online]. Available: https://cacm.acm.org/magazines/1999/5/7905-credibility-and-computing-technology/fulltext
19. L. Festinger, *A Theory of Cognitive Dissonance*. Stanford, CA: Stanford Univ. Press, 1957.
20. A. Marantz, *Antisocial: Online Extremists, Techno-Utopians, and the Hijacking of the American Conversation*. New York: Viking, 2019.
21. S. Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. London: Oxford Univ. Press, 2018.
22. M. Isikoff and D. Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. New York: Twelve Publishing, 2018.
23. R. Mueller, "The Mueller Report: The final report on the investigation into Russian interference in the 2016 presidential election," U.S. Department of Justice, Washington, D.C., 2019.
24. A. Yurchak, *Everything Was Forever, Until It Was No More: The Last Soviet Generation*. Princeton, NJ: Princeton Univ. Press, 2005.
25. FiveThirtyEight, "2016 election forecast," 2016. [Online]. Available: https://projects.fivethirtyeight.com/2016-election-forecast/
26. Election Projection, "2020 election projection polls." Accessed on: Oct. 10, 2019. [Online]. Available: https://electionprojection.com/latest-polls/presidential-polls.php.
27. Federal Elections Commission, "Federal Elections 2016: Election Results for the U.S. President, the U.S. Senate and the U.S. House of Representatives," Washington, D.C.,Dec. 2017. [Online]. Available: https://transition.fec.gov/pubrec/fe2016/federalelections2016.pdf.
28. D. Wasserman, "2016 national popular vote tracker: Overall vote." Accessed on: Oct. 10, 2019. [Online]. Available: https://docs.google.com/spreadsheets/d/133Eb4qQmOxNvtesw2hdVns073R68EZx4SfCnP4IGQf8htmlview?sle=true#gid=19.
29. USC Annenberg School for Communication and Journalism, "How Russian Hackers & Trolls Exploited the U.S. Media in 2016," YouTube video, 56:26, October 4, 2018, https://www.youtube.com/watch?v=H1WW0yQOtuo.

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.