I invited Phil Howard and Gillian Bolsover in November of 2016 to guest edit this special issue of *Big Data* on “Computational Propaganda.” I am delighted at the collection of academic papers that they have curated on the subject, which is front and center at the moment. Politicians, journalists, and scholars grapple with how and to what extent social-media platforms were used to manipulate the presidential election of the oldest democracy in the world.

While the details were murky last year, it was becoming evident to us at *Big Data* that we were witnessing the vulnerability of social media for political mass manipulation for the first time. Despite a large-scale scientific study* conducted by Facebook in 2012 demonstrating that users’ moods could be manipulated via messages fed to its users, it continued to maintain a position of “algorithmic neutrality” on content. Other reports in the media had suggested that it was difficult for most people to distinguish humans from bots on Twitter. While the evidence suggested that social-media platforms were ripe for manipulation, the platforms didn’t seem particularly worried about the potential consequences of the research findings. A year later, however, with increasing evidence of manipulation, it is time to ask ourselves whether we need to make some changes to preempt potentially worse consequences going forward, namely, the potential for digital platforms being used as weapons by malicious actors. Common sense would suggest that we do, and while there are no easy answers, we need to start asking ourselves whether our liberal free-market values are vulnerable to rogue governments or groups who are able to sow havoc using minimal financial resources. We need to start finding answers.

The Facebook study of 2012 had indeed sparked outrage and concern around the use of data for social experimentation without consent of human subjects. It was worrisome that data-usage policies of virtually all digital platforms had become increasingly rapacious over the years, allowing them to do what they please with the data they collect assiduously. Facebook’s social experiment would never have been approved by an Institutional Review Board (IRB) for university research involving human subjects. But the outrage resulted in nothing. There was no regulatory body, and there still isn’t one that addresses unethical use of data by business entities, even though the implications are arguably as serious as those involving national security.

Facebook’s research, conducted with a great deal of rigor on a large scale, clearly demonstrated that their users could be manipulated on their platform. Would this public knowledge not induce a motivated party to exploit such vulnerability, especially if the stakes are high and the costs low? The U.S. government is well aware that it has no shortage of overt and covert enemies. So, why would it not take steps to thwart them on digital platforms in the same way as it attempts to do so in other arenas? The very real possibility that a party with meager resources can potentially derail a vibrant democracy at virtually no cost represents an incalculable “externality” imposed on us through a known vulnerability in our digital ecosystem.

In a recent article on “FinTech” platforms,† my coauthor and I point out that because trust is so important when it comes to our money, we have historically held banks and financial firms to much higher standards of compliance and control than other businesses. Financial institutions are required to follow well-defined processes, with oversight and fail-safe plans aimed at minimizing risk and maximizing public trust. The terror attacks of 2001 ushered in stringent “know your customer” (KYC) regulations, requiring that such institutions know their customers in great detail. The 2008–2009 crisis resulted in even more stringent regulation aimed at mitigating economic instability and curbing the use of funds for financing terrorism and other illicit

---

*I http://www.pnas.org/content/111/24/8788.full

†https://cacm.acm.org/magazines/2017/10/221331-fintech-platforms-and-strategy/fulltext
activity. This regulatory burden comes at considerable cost to us, but we require it for our societal well-being.

In contrast, the news industry is expected largely to regulate itself. Indeed, we pride ourselves on our freedom of the press, and the freedom of expression. Indeed, one of the wonders of the Internet era is the empowerment of individuals as publishers on digital platforms. However, unlike news organizations whose reputations ultimately depend on careful verification, we have allowed digital platforms to function without any damages for publishing material that is harmful to society, as long as their consumers are delighted by it. They are now promising us they will do better in the future by employing more people for fact checking. Would we have trusted the bankers with such a promise after the financial crisis and left them alone to regulate themselves? Why is tech so special?

An important lesson we have learned from the rise of digital platforms is that they disrupt industries by blurring the boundaries between them. Which industry does Amazon belong to? What about Google? Facebook? Apple? The answers are increasingly vague. And yet regulation continues to be siloed largely by industry, like finance, retail, and telecommunication, despite their increasing irrelevance in classifying some of our largest and most powerful businesses. KYC is critical to finance because every industry uses financial services. I would argue that digital platforms have become similarly ubiquitous to virtually every industry and should demand equally stringent regulation if not more so.

For starters, KYC requirements should be considered for digital platforms similar to those for financial institutions. Advertisements on mass media are plain for everyone to see, and political ads require disclosing who paid for them. Yet, in the narrowcasting world of digital targeting, it is possible for parties to target individuals with customized hate-speech ads completely under the radar without the public or regulators ever noticing, or even without the platform designers being aware of their algorithms being used in ways they had never envisioned or intended! We cannot trust digital platforms with self-policing such a role, since it is in conflict with their primary goal of maximizing shareholder value. Mission statements such as “give people the power to build community” are not the responsibility of profit-maximizing entities, and the sooner regulators and governments recognize it the better.

Requiring KYC requirements on digital platforms is not new. AirB&B already does an automated KYC in real time through verification of government issued IDs. Social-media platforms could be required to do something similar but with the added restriction of requiring foreign publishers to obtain legitimate U.S.-issued IDs to advertise in the United States. This would pre-empt the use of legitimate identities issued by governments who may be sponsors of illicit activity or harmful propaganda.

Second, we need better guidelines around the ethical use of data, especially around profiling and social manipulation. Business must follow IRB policies around the use of human subjects for social experimentation, just as university researchers are required to follow, regardless of their stated data-usage policies, which most individuals don’t even read let alone understand. For too long, regulators have turned a blind eye to the use of data, emboldening digital platforms to do as they please with no oversight. A recent proposal allows users to take action if they find unwanted inferences are being drawn about them—understanding on what data the inferences are based and even allowing users to “cloak” their personal data—but this requires them being aware of such inferences about them in the first place. We need something more pre-emptive where data-rich companies disclose broadly their data-mining goals and policies and demonstrate that they are not violating the implicit intentions of users who entrusted them with their data.

There are no easy answers, but turning a blind eye to this new Internet phenomenon will continue to expose us to considerable peril in the future. The U.S. government and our regulators need to understand how digital platforms can be weaponized and misused against its citizens, and equally importantly, against democracy itself.