

Social Engineering via Predictive Algorithms

You Voted Obama, You Voted Trump, You Voted for X [?]

Sebastian Esteva

Winter 2023

What book inspired your current career path? Which great artist's work has deeply impacted your life? What is an experience that shaped you into who you are today? While it's easy to point out key moments of your life, algorithms can be fine-tuned to identify and manipulate aspects of your life you never knew were impacting you. And as computing technology exponentially improves, the power of algorithm's have become so complex that "...not even the engineers...who create the algorithm can understand or explain what exactly is happening inside them..." (IBM). And, in our creation of ever-better algorithms, our lives have become increasingly filtered and dictated by them. These algorithms are coming under increasing scrutiny after the viral 2020 documentary the Social Dilemma, along with a plethora of scandals such as that which arose from Cambridge Analytica. This paper will show how effective and powerful algorithms are at targeting people and how they can change our minds through extreme social engineering. Furthermore, I will analyze how algorithms have, and will potentially, add new levers of imperceptible control upon people bringing about a considerable shift in citizenship.

To begin, let us go back to 2008 USA when Obama, for the first time in campaign history, made use of mass data and direct-to-voter communication technology. For instance, Obama dominated direct texting, with 17% of Obama supporters getting direct messages from the campaign compared to 7% of McCain supporters (Smith). In 2008 this technology was touted as having real potential to not only spread a message but also get people out voting as "...[people] who received a reminder in a text message one day before an election were 4.2 percent more likely to vote" (Stelter). Another innovation of Obama's campaign was to send trial batches of emails with different subject lines to see which emails would get high response

rates (Aaker). They even specialized their messages to resonate regionally (Chang). In fact, Obama did such an excellent job in getting his message out there, that in 2008 he was the first politician to get Advertising Age's marketer of the year award (Michaelsen). More crucial than receiving Advertising Age's oh-so-prestigious award was Obama's successful campaign for the presidency. A victory Arianna Huffington, chief editor of the Huffington Post, said this about, "Were it not for the Internet, Barack Obama would not be president. Were it not for the Internet, Barack Obama would not have been the nominee" (Miller). Arianna's claim may be exaggerated, but she is making this claim not only for the publicity which Obama enjoyed on the internet but because of how his campaign harvested data to create more effective and personalized outreach and get-out-the-vote campaigns. I share this as a tangible example of how even technology from over a decade ago facilitated nudging and recruiting people to get someone elected to the most powerful position in the world. Now algorithms can do everything the Obama campaign did and much more.

How Algorithms Contribute to Social Engineering: Data Collection and Profile Generation

First, algorithms can mine data and create shockingly accurate profiles of individuals. For instance, online security companies are considering implementing technology that continually authenticates a computer's user based on how they are using their mouse and keyboard (Hu). Some people may feel safe from targeting algorithms since they limit the direct information they share to a social media site or general website. However, algorithms can create a profile of you with minuscule bits of information; sharing more just solidifies that picture. For example, likes on Facebook can accurately predict "...gender, sexual orientation, race, ethnicity, religious beliefs, political views, relationship status, intelligence, use of addictive substances, and even the marital status of one's parents," writes Sarah Bender from the Mitcham Law review. Tools such as these offer ripe fruit for any resource-rich individual (company or person) to exploit. Moreover, algorithms impact reach into the physical world, as can be seen by algorithms trained to recognize people based on their gait and silhouette, removing the need for a clear image of an individual's face or other biometric information (Kumar). This alone could be a potent tool for authoritarian regimes to identify and persecute resistance, something China is already doing (ABC News). Algorithms can even know things about us that we do not, as with the famous case from ten years ago when Target's advertising algorithm, which the company dumbed down after this incident, knew a woman was pregnant before she did (Hill).

The most famous example of data gathered and compiled by algorithms in use today is Cambridge Analytica. The company's algorithms create psychographic profiles that gauge people's agreeableness, neuroticism, openness to new experiences, extroversion, and conscientiousness. An estimated 87 million non-consenting individuals' data was profiled in this manner (Chadwick). Cambridge Analytica sold this data for many purposes, but to focus on the political side, they were selling the ability for politicians to tailor their pitches from person to person (Detrow). However, Cambridge Analytica's software seems to be something other than the promised silver bullet, with Ted Cruz's presidential bid phasing out the use of the technology after being unimpressed by its results. However, Analytica's profiles DO seem to be the silver for the magic bullet with only a need for proper craftsmanship, especially as numerous studies, such as that conducted by Dr. Zarouali of Amsterdam University, have shown that citizens are more persuaded by political ads that match their personality traits.

The 2016 Trump campaign is an example of effective use of Cambridge Analytica. They used the data provided to decide where Trump should campaign and where, when, and how it should advertise (Cadwalladr). Nevertheless, its use is less heavily credited for his win than Obama's use of technology in 2008. This is likely because all campaigns now use technology to high levels of sophistication, and so the gap between Trump and Hillary was less dramatic than that between Obama and McCain. This spawns the argument that algorithms are not damaging citizens' access to power structure; if anything, they are just extending the reach of politicians' messages to citizens, encouraging more participation in government. This is a valid point; however, what does that look like when a politician wants to create a smear campaign? Or when a foreign state wants to manipulate our elections more effectively? Or when a non-democratic state now has a tool to entrench its voice?

Algorithms implemented to mine data on individuals, such as the examples stated above, serve primarily to empower large conglomerates (like the state or companies). This is due to larger institutions interacting with a greater total population size, and therefore benefiting the most from understating who is who and then being able to tailor their work with greater sophistication. For instance, the net impact of the Democratic party knowing their entire voting bases' psychosocial profile and then being able to target their messaging accordingly is quite large. We know this through the Obama Campaign, where data-informed messaging was a crucial component of the election. Compare this to you and your work friend Darell. A computer telling you that he has an A-type personality stands to gain you little. Partially

because what benefit is there to you adjusting your behavior for Darell and also because you already know Darell's personality by virtue of knowing him without a computer telling you. These large-scale data mining algorithms of individuals suddenly give institutions which never would have known you personally the ability to do that in a pseudo fashion. This sounds positive on its surface. However, this natural progression threatens to turn Mill's marketplace of ideas into a personal theater, projecting a reality filtered to satisfy you. Dr. Zuboff, a Harvard professor, has rung the warning bell on this saying, "[algorithms] ...effects are felt in the real world, where they splinter shared reality, poison social discourse, paralyze democratic politics...". Thus, not only do data algorithms re-defined the relationship between citizens (a relationship shift that benefits them more than us), the hyper-individualized world (which is possible only with this data) divides us. Citizens are further shaken by the algorithm's other power— manipulation.

How Algorithms Contribute to Social Engineering: Manipulation

Excluding language, Algorithms are unequivocally the best manipulation tools ever created by humankind. Furthermore, their effect can be profound when combined with the information-gathering algorithms discussed above, as their effectiveness scales with the amount of data available to them. In, "Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy," Dr. Taylor Owens reports on several of his experiments, which showed that algorithms could influence people's political and dating decisions through explicit and covert tactics. This is a significant threat specifically to citizenship, as it gives those with access to the technology a form of highly potent propaganda. Professor Stuart Russell, a computer scientist at UC Berkeley, put it this way "...Algorithms have more control over human cognitive input than any dictator in history..." (Williamson). The use of propaganda to influence has been a key component of governance since the dawn of time, and it has only grown in sophistication since the Cold War. However, increased media literacy and a free press can act as suitable countermeasures to these tactics. But, there may be no way for us to resist algorithm's powers completely since "Sophisticated manipulation technologies have progressed to the point where individuals perceive that decisions they make as their own, but are instead often 'guided' by algorithms..." (Manheim). Suppose this technology was to approach wide-use adoption in political fields, which it inevitably will if no action is taken, as those who do not use it would be left behind (like McCain). The success of a political campaign could end up relying more heavily on who's algorithm was best tuned, and less on their

message. Authoritarian states would have a tool capable of not only pacifying but effectively gaining support from their citizens. All of this with the individual thinking their decisions were their own.

A persuasive counter to these arguments is that these algorithms are, at times, only marginally effective. For instance, Facebook found that it could increase voter turnout by .39%, which is a minuscule percentage (Kramer). However, once the other factor of the algorithm's powers come into play, their ability to act on a huge scale makes those numbers far more impressive. That .39% of people encouraged to vote translated to 340,000 votes according to Facebook researchers. If this technology were applied strategically to increase or suppress the vote, whole elections could be engineered. To put the potential power of this into perspective, Biden won Arizona over Trump in 2020 just by 10,457 votes, and many elections in the US hold those thin margins of victory (CNN). Meaning, people with algorithmic power could have a significant impact in swinging close elections, a tactic history shows us can have huge effects. The Anti-Saloon League being a prime example of this, as they successfully played tight margins to push the US into the 18th amendment (Okrent 35).

Algorithms do not have the power to force you to act against your will; they shape your will. Thus, our position in society (being a citizen) has the potential to shift away from being a partnership into a union where the wielder of the algorithm holds outsized power over the citizenry. And, if an algorithm can not shape your will, rest assured a more vulnerable target is out there. For instance, individuals swept up in the Q-anon conspiracy. In fact, Q-anon is an excellent example since it grew partly because of Facebook's and YouTube's algorithms indoctrinating people into it as they attempted to follow their programming and maximize platform engagement (McNamee). And the frightening thing about that is that those algorithms amplified those conspiracies under no specific direction.

The Aggregate Effect on Citizenship

Algorithms know you, and algorithms can be used to shape you. And so these marvels of technology we have created will profoundly shift the core of citizenship, an individual's relationship to the greater society. For at their heart, all definitions of a citizen revolve around an individual and how they should act in society, whether that be Hobbes's belief in surrendering power to a dictator or Madison's view in Federalist Paper Ten to segment society. And it is that very relationship that algorithms threaten to shake up.

In societies where the individual is enshrined, such as the USA, algorithms will assist in separating us. We can imagine these algorithms working from the bottom up, fracturing society into continually shrinking bubbles, as messages become targeted not at a state, city, or even a specific group of society, but you. The only logical progression is the re-defining of the citizen's relationship with a larger power structure and one another. The exact tract of such a shift is hard to pin down. However, its consequences of reduced productive discourse between one another as our exposure to opposing views, and tolerance of them, plummets seems to be the trajectory of the (currently) unregulated industry. Another parallel shift in such individualistic societies would be the addition of a powerful tool in the hands of the leaders to no longer "...adjusts and ...[change], shifting to absorb new people and ideas", which the Chairman of the Joint Chiefs General Mark Milley claimed to at the heart of a healthy liberal democracy, but rather to precisely manipulate the masses (Applebaum). This is an action that societies which value uniformity, such as China, would likely implement more explicitly. The state will be able to dictate a common goal from a set of ideals to an algorithm to proliferate among its citizens, strengthening their relationships with greater society. This ability of influential figures and/or the state to manipulate human decisions brings up a deeply philosophical debate about when our choices are no longer our own. At what point does our relationship with society, our role as citizens, cease to hold meaning? If independent choices are a crucial aspect of that position, then societies globally are moving into a huge upset.

Imagine if that book that inspired your career, if that great artist whom you stumbled upon, were placed there by an algorithm. Or, if all those little moments which make you who you are just became knobs and data points to be turned by the will of whoever has the most powerful algorithm. For you know whom you voted for yesterday, but how confident are you that tomorrow you will truly be the one filling in the bubble to vote for X? Does that even matter to you as a citizen?

Works Cited

Aaker, Jennifer, and Victoria Chang. "Obama and the Power of Social Media and Technology." Stanford Graduate School of Business, 2009, <https://www.gsb.stanford.edu/faculty-research/case-studies/obama-power-social-media-technology>. Accessed 2 March 2023.

- Andriole, Steve. "A Few Moments From This Week at the White House." YouTube, 29 January 2022, <https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy--effective/?sh=6516699a6781>. Accessed 4 March 2023.
- Applebaum, Anne. "Democracies Don't Try to Make Everyone Agree." The Atlantic, 2021, <https://drive.google.com/file/d/15sfGdeF8Yn7ICwqK21i9Qrhavr6t5OjM/view?usp=sharing>. Accessed 2023.
- Bender, Sarah ML. "Algorithmic Elections." Michigan Law Review, December 2022, <https://michiganlawreview.org/journal/algorithmic-elections/>. Accessed 2 March 2023.
- Bianchi, Tiago. "Global search engine desktop market share 2022." Statista, 6 January 2023, <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>. Accessed 21 February 2023.
- Cadwalladr, Carole. "How Trump Consultants Exploited the Facebook Data of Millions (Published 2018)." The New York Times, 17 March 2018, <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Accessed 3 March 2023.
- Chadwick, Paul. "How many people had their data harvested by Cambridge Analytica?" The Guardian, 16 April 2018, <https://www.theguardian.com/commentisfree/2018/apr/16/how-many-people-data-cambridge-analytica-facebook>. Accessed 3 March 2023.
- "Chinese authorities use 'gait' surveillance to identify people by their body shape and walk." ABC, 6 November 2018, <https://www.abc.net.au/news/2018-11-06/chinese-gait-recognition-tech-ids-people-by-how-they-walk/10469974>. Accessed 2 March 2023.
- CNN. "Arizona Election Results and Maps 2020." CNN, 2020, <https://www.cnn.com/election/2020/results/state/arizona>. Accessed 4 March 2023.
- Detrow, Scott. "What Did Cambridge Analytica Do During The 2016 Election?" NPR, 20 March 2018, <https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>. Accessed 14 March 2023.
- Fogg, B.J. Persuasive Technology: Using Computers to Change What We Think and Do. Elsevier Science, 2003. Accessed 4 March 2023.
- Hill, Kashmir. "Home." YouTube, 2012, <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4c63da2b6668>. Accessed 2 March 2023.
- Hu, Teng. "An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning." Hindawi, 2019, <https://www.hindawi.com/journals/scn/2019/3898951/>. Accessed 2 March 2023.
- IBM. "Explainable AI (XAI)." IBM, <https://www.ibm.com/watson/explainable-ai>. Accessed 4 March 2023.
- Kramer, Adam. "Experimental evidence of massive-scale emotional contagion through social networks." 2014. PNAS, <https://doi.org/10.1073/pnas.1320040111>.

- Kumar, Munish. "Gait recognition based on vision systems: A systematic survey." *Science Direct, Elsevier*, February 2021, <https://doi.org/10.1016/j.jvcir.2021.103052>. Accessed 2022.
- Manheim, Karl. "Artificial Intelligence: Risks to Privacy and Democracy." *Yale Journal of Law & Technology*, 24 April 2019, https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf. Accessed 4 March 2023.
- McNamee, Roger, and Daily Kos. "Facebook is driving QAnon's growth and enhancing its power." *Los Angeles Times*, 30 September 2020, <https://www.latimes.com/opinion/story/2020-09-30/facebook-k-qanon-conspiracy-social-media-election>. Accessed 14 March 2023.
- Michaelsen, Abigail. "Brand Obama: How Barack Obama Revolutionized Political Campaign Market." *Claremont McKenna College*, 2014, https://scholarship.claremont.edu/cmc_theses/990/. Accessed 2 March 2023.
- Miller, Claire. "How Obama's Internet Campaign Changed Politics." *New York Times Archive*, November 2008, <https://archive.nytimes.com/bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics/?smid=pl-share>. Accessed 2 March 2023.
- Okrent, Daniel. *Last Call: The Rise and Fall of Prohibition*. Scribner, 2010.
- Owens, Taylor. "Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy." *Data Governance in The Digital Age*, 2018, pp. 70–91. JSTOR, <https://www.jstor.org/stable/resrep26128.7>. Accessed 4 March 2023.
- Shelton, Kelly. "The Value Of Search Results Rankings." *Forbes*, <https://www.forbes.com/sites/forbesagencycouncil/2017/10/30/the-value-of-search-results-rankings/?sh=534fcbfe44d3>. Accessed 21 February 2023.
- Smith, Aaron. "The Internet's Role in Campaign 2008." *Pew Research Center*, 15 April 2009, <https://www.pewresearch.org/internet/2009/04/15/the-internets-role-in-campaign-2008/>. Accessed 5 March 2023.
- Stelter, Brian. "Enticing Text Messagers in a Get-Out-the-Vote Push (Published 2008)." *The New York Times*, 17 August 2008, <https://www.nytimes.com/2008/08/18/us/politics/18message.html>. Accessed 2 March 2023.
- Warzel, Charlie. "Is Google Dying? Or Did the Web Grow Up?" *The Atlantic*, 20 June 2022, <https://www.theatlantic.com/ideas/archive/2022/06/google-search-algorithm-internet/661325/>. Accessed 21 February 2023.
- Williamson, Chris. "Social Media Algorithms Are Manipulating Human Behaviour." *YouTube*, 27 August 2021, <https://youtu.be/OrPJmntsHww>. Accessed 4 March 2023.
- Zarouali, Brahim. "Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media." *Sage Journal*, vol. 49, 2020, pp. 1066–1091. *Journals Sage Pub*, <https://journals.sagepub.com/doi/pdf/10.1177/0093650220961965>. Accessed 2023.