Social Engineering

How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication

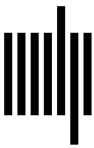
By: Robert W. Gehl, Sean T Lawson

Citation:

Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication
By: Robert W. Gehl, Sean T Lawson
DOI: 10.7551/mitpress/12984.001.0001
ISBN (electronic): 9780262368926
Publisher: The MIT Press
Published: 2022

OA Funding Provided By:

OA Funding from MIT Press Direct to Open



The MIT Press

8

Conclusion: Ameliorating Masspersonal Social Engineering

In this book, we took up the call from several people to consider emerging forms of manipulative communication as social engineering. In doing so, we argued that there is, indeed, a strong affinity between the concept of social engineering and the mixture of practices such as email hacks, meme production and sharing, attempts to microtarget voters, and social media pretexts. Not only are these practices the descendants of mass social engineering and propaganda developed in the early twentieth century, they are also related to the hacker practice of interpersonal con artistry.

We have deployed a critical approach to strategic communication through the use of concepts derived from hacker studies. This leads to a new understanding of our contemporary digital media environment. After tracing the threads between mass and hacker interpersonal social engineering, our penultimate ambition was to reveal elements of trashing, pretexting, bullshitting, and penetrating in two key events: the Russian election interference campaign and the use of psychographics by Cambridge Analytica to sway public political opinion. These were indications of what security researcher Thomas Rid calls "political engineering, social engineering on a strategic level."[1] These events—and many others like them

that we still experience—saw hacker social engineering scaled up to societal level, and thus approaching the ambitions of the older mass social engineers to penetrate media markets or large-scale social institutions.

We hope that our work shows that the relationship between targeted, interpersonal social engineering and mass social engineering is fluid. This may help us overcome impasses in current analyses of manipulative communication practices, including those of firms like Cambridge Analytica. Do targeted, interpersonal techniques work? Or should we be more concerned about mass messaging? A 2020 debate held between two important scholars of political communication, Emma Briant and David Karpf, pitted these two perspectives against one another, with Briant taking up the argument that psychographic targeting of individuals is a dire threat to democratic deliberation, and Karpf expressing more concerns about mass messaging. To be fair to both of them, the debate was structured so that they had to simplify their positions by taking these opposing sides. However, if the debate was meant to resolve the impasse, it did not. Briant maintained that precise targeting is the most dangerous development in recent political communication, and Karpf argued that mass communication is still dominant in political communication.[2]

By bringing hacker concepts to bear on mass social engineering, and by bringing the results forward to our current media landscape, we may be able to avoid such mass/targeted impasses. After all, the mass social engineers saw themselves as crowdmasters—that is, interested in mass communication to convert unruly crowds into manageable publics. The hacker social engineers targeted individuals or, at most, organizations. If the two types of social engineering have many overlaps, then it is wise to speak of *masspersonal* social engineering, where social engineering can easily slide from large-scale campaigns to hyper-targeted individual hacks and back again, depending on the target to be penetrated, the interactions

the social engineer seeks to have with the target, the specific goals the social engineer wants to achieve, and the specific platform or medium used for communication.[3] Our concept of masspersonal social engineering conforms to observations that our contemporary, digital media environment is a masspersonal communicative one.[4] The existence of a fluid form of masspersonal social engineering is supported by our analysis of the IRA and Cambridge Analytica practices, both of which oscillated between targeted and mass communication and relied on the techniques of trashing, pretexting, bullshitting, and penetrating.

But some questions remain. First of all, is masspersonal social engineering effective? For example, the burning question after the 2016 US election was, of course, did the Russians get Trump elected? Or was it Cambridge Analytica? Or something else? To be blunt, we don't think we can answer this question, but our analysis of masspersonal social engineering can provide clues, as we will discuss.

Second, can masspersonal social engineering be ethical? Throughout this book, we have discussed some disturbing examples of social engineering: blaming unionists for a fire that killed children; increasing smoking among women; covertly listening in on people's phone calls; breaking into computer networks; discouraging Black Americans from voting; using ill begotten data to craft highly targeted fear appeals; sowing chaos in the democratic process. Are there cases in which the coordinated use of trashing, pretexting, and bullshitting can be put to good penetrating use? To be blunt again, we don't think so.

Finally, what is to be done about masspersonal social engineering?

Is Masspersonal Social Engineering Effective?

There remains the question of whether masspersonal social engineering works. Our key cases have been the Russian election

interference operation and the microtargeting political communication of Cambridge Analytica. Did either affect the US presidential election? Has the combination of big data, social media, and psychological sciences been able to deliver on the longstanding dream of precise, direct effects of communication?

Despite all the documentation of these events, academics and journalists are still trying to figure this out. For example, Kathleen Hall Jamieson's book, *Cyberwar*, emphatically argues that the Russian masspersonal social engineering campaign did work, setting the agenda for debate and swaying undecided voters in key swing states.[5] Similarly, the UK's *Channel 4* investigative report into Cambridge Analytica's use of data to help the Trump campaign argues for a correlation between their efforts to deter Black voters from voting and the reduced turnout among Black voters in key states like Wisconsin.[6] "We can't know what effect these ads had on each voter that saw them," the report notes, "but for the first time in 20 years, Black turnout fell."[7] Such efforts dovetail with the Russian pretexts of Black Lives Matter activists who repeatedly stated that voting was a useless gesture for Black Americans. The fact that Black voting was down in states like Wisconsin and Michigan lends some credence to the argument that such masspersonal social engineering worked.

However, there are strong arguments against this claim. For example, the Cambridge Analytica skeptic David Karpf argues that "Donald Trump's campaign didn't possess a secret data innovation. His unlikely victory was due to a messy confluence of factors," including a poor campaign by Clinton (she infamously did not campaign in Wisconsin during the general election), James Comey's announcement that the FBI was going to investigate Clinton's email server eleven days before the election, and old-fashioned sexism.[8] As for Russian interference, Harvard Law professor Yochai Benkler argues that "we should remain skeptical that Russians spending a couple of hundred thousand dollars on Facebook advertising had

meaningful impact relative to a presidential campaign spending millions of dollars while being guided by Facebook's own marketing team."[9] Similarly, Thomas Rid, a leading scholar of cyber conflict, argued that it was "unlikely that the trolls convinced many, if any, American voters to change their minds" or "had any discernible effect on the voting behavior of American citizens."[10] Russia might have sought to help the Trump campaign, but Trump was also, in fact, campaigning, and it is too reductive to suggest the tens of millions who voted for Trump were duped by Russia.

The debate about the effectiveness of Cambridge Analytica or the IRA will no doubt continue to rage. We ourselves are not in a position to decide if either were successful. Our purpose is to conceptualize masspersonal social engineering. But in doing so, we find the need to sound three warnings.

First, over and over again in the information security literature, we find reports that *hacker* social engineering—the interpersonal trashing, pretexting, and bullshitting—is extremely effective in achieving the social engineer's goal of penetrating information systems.[11] This claim is not disputed. If highly targeted, interpersonal social engineering is effective, this suggests that messages customized for particular groups of targets—say, one of the thirty-two personality types theorized in the OCEAN psychographic system—may very well be effective, so long as the messages are based on extensive trashing, have pretexts that are recognizable to targets, and include carefully crafted bullshit. This would of course take incredible effort, but the success of interpersonal social engineering indicates that such a masspersonal campaign has the real potential to be effective.

We are aware that this warning reflects a longstanding assumption about the instrumental approach to communication: direct effects might not work just yet, but with advancements in technologies for data collection and targeting, one day we would be able to achieve such effects. From the days of mass social engineers Lee,

Bernays, and Fleischman to the present, a recurring dream has been about the advances in communication technologies and social science theories leading to a deeper and more accurate penetration of the minds of audiences. What we're suggesting here, however, is not that advances in technology will inevitably lead to the realization of the dream of direct effects. Instead, we're suggesting that future masspersonal social engineering may better implement the successful model of interpersonal hacker social engineering on a large scale. At that point, Cambridge Analytica or the IRA's efforts may seem to be clumsy approximations of those efforts.

Our second warning: our analysis of hacker social engineers shows that their success in gaining access to restricted systems stems from repeated efforts. For example, the hacker social engineer Kevin Mitnick's recollection of his social engineering attack on Motorola in the 1990s is marked by many, many phone calls to many employees—with a variety of pretexts—until he was able to find an employee who could give him access to the source code of a new cell phone.[12] This highly iterative approach is predicated on the fact that the social engineer's pretexts and bullshit won't work on everyone in a given organization, but that they will work on at least one person. That such repeated efforts have been scaled up in contemporary digital media should come as no surprise. Phishing emails operate on this principle. Likewise, digital advertising—which measures success in tiny increments—also reflects this principle. This alerts us to the fact that, in the case of masspersonal social engineering, if an entity is allowed to continue trashing, pretexting, and bullshitting a given target, it will find vulnerabilities in that target. And when the target in question is a large swath of society, there are many opportunities to attack it over and over again. If, for example, the target is a population that has some preexisting distrust in government institutions, and a masspersonal social engineer repeats messaging undermining faith in a particular governmental practice—say, conducting an election, addressing a pandemic, or

preventing climate change—then the likelihood of success starts to rise. Russia's continuous efforts over the past several years are strikingly similar to Mitnick's repeated phone calls.

Finally, social engineering is not the only technique for shaping society. Again, to use hacker social engineering as a source for clues, hacker social engineers don't just rely on interpersonal con artistry. They can couple that with technical attacks—the most common connotation of "hacking"—such as exploiting software or network flaws. Likewise, organizations seeking to shape an election have more tools than just masspersonal social engineering at their disposal. In the case of Donald Trump and the Republican Party's work to suppress Black voting, voter ID laws, gerrymandering, and challenges to ballots from predominantly Black population centers have been effective techniques and can be used in concert with masspersonal social engineering efforts to suppress minority voting. Messages coming from Republican masspersonal social engineers are also amplified in what propaganda scholars call the "right-wing media ecosystem," including outlets such as Fox News, which has parroted the idea that votes coming from predominantly Black population centers should be suspected as fraudulent.[13] While we may or may not be able to tell if Cambridge Analytica's or Russia's efforts to suppress Black voting were successful, we can say without a doubt that they were done in concert with these other practices. And when it comes to the Russian effort, they are obviously not limited to masspersonal social engineering; Russian intelligence organizations have also hacked election systems.[14]

However, despite these warnings, we also accept the possibility that there is simply no way to effectively expand hacker social engineering to a mass scale, that there is some boundary between an interpersonal con job and the manipulation of a society. In fact, as we will discuss below, we ourselves subscribe to the vision of communication as the mutual constitution of reality—beset by struggles, to be sure, but fundamentally about the voices of people

who seek to understand themselves and their worlds and, in doing so, associate together for the good of all. From this viewpoint, if efforts at masspersonal social engineering are not effective, another possible explanation could be that the fundamental assumptions about communication made by Russian operatives or political consultancies were always too simple and linear. Perhaps we still fail to achieve the dream of direct effects because, as critics have noted for decades, the role of communication in society and culture is not as simple as changing individual minds that then add up linearly and predictably into a mass. Perhaps the role of communication in society and culture is more complex and given to nonlinearity, feedback, dissensus, and emergence than the masspersonal social engineers would have us believe. It could be the case that an interpersonal hacker social engineer could fool a few of us for some of the time, but there could be no way for masspersonal social engineers to fool many of us, all of the time.

But we should be clear. None of this means that masspersonal social engineering or other forms of social engineering don't have effects. Perhaps they are not the effects that their users have so often dreamed of having. Just because they might not do what was intended, that doesn't mean they do nothing at all and that the effects they do have aren't potentially negative.

There are many examples of sociotechnical developments that did not have particularly great immediate effects or, in some cases, did not really work at all, but which are now recognized as having been vitally important despite (or perhaps because of) their failures. Since one of the penetration metaphors social engineers rely upon is that of the bullet, some military analogies are, perhaps, in order. We can think, for example, of historical analysis of the ironclad Civil War-era military ship the USS *Monitor* which argues that the ship was largely a failure as a warship but a resounding success in terms of the publicity it generated, as well as in its status as a powerful vision for the future of naval warfare.[15] Much later,

during WWII, Norbert Wiener's "anti-aircraft predictor" failed as an effective anti-aircraft weapon but succeeded in sparking a "cybernetic worldview" that became the core of our understanding of the so-called Information Age.[16] In the postwar period, a preeminent historian of technology points to another "failed" weapon system for its important, long-term implications: the SAGE air defense system. Again, though the system did not really succeed at its primary mission of mitigating the Soviet nuclear threat, it was an important forerunner to the emergence of the internet.[17] Finally, we can look to Operation Igloo White during Vietnam. This was an effort to use electronic surveillance and precision airstrikes to stop infiltration along the Ho Chi Minh Trail. It didn't work. But the vision it inspired of intelligence-driven, precision targeting found a home in US military thinking from the 1980s on.[18] The details of these cases vary, but a pattern appears: the initial efforts to deploy the new weapon system largely failed, but in that failure, participants and observers alike were left with the question: But what if it had worked? What if we made some modifications and tried harder next time? Entire sociopolitical systems were built around these failures in order to achieve their intended effects.

We should expect nothing less with respect to masspersonal social engineering. Indeed, doubts about the effectiveness of the Russian effort to affect the 2016 US presidential election didn't stop the Russians from trying again in the mid-term elections of 2018 and the presidential election of 2020. Rather than fretting about whether or not Cambridge Analytica's targeting efforts worked, successors to that firm, like Phunware or Rally Forge, plowed ahead with their own efforts. These continued examples of attempted manipulation along the lines of what happened in 2016 indicate that there are plenty of people still striving to get masspersonal social engineering to work. Even if it fails, the effects of masspersonal social engineering can include renewed efforts at manipulative communication.

Moreover, if the stated purpose of these efforts was to sow distrust in institutions, the response to the COVID-19 pandemic and the insurrection attempt of January 6, 2021 indicate that the mission may well have succeeded. Therefore, we strongly suggest continued analysis of the efforts of masspersonal social engineers, whether they are effective or not.

Can Masspersonal Social Engineering Be Ethical?

A second question: can social engineering ever be used for good?

Throughout this book we have relied heavily on the insights of people who refer to themselves as "ethical social engineers." Sharon Conheady, Jenny Radcliffe, and Chris Hadnagy identify this way, offering their hacking services to organizations who want to test their security. Even the reformed felon hacker Kevin Mitnick offers his services as an ethical hacker.[19] These people most definitely engage in social engineering by our definition. They trash; they create pretexts; they bullshit; and they penetrate.

But, as we discussed in chapter 6, the fact that these social engineers report on their activities tells us something is different about ethical social engineering for penetration tests. There comes a point when the hacker drops the pretext, resumes their professionalized persona, and provides a report of their penetration test. Ideally, at that point, the organization can learn from the experience and offer training to employees. All of the elements of social engineering are in place, but only for a limited period of time, and the intention is always to reveal any deceptive practices to victims.

Something similar could be said about efforts to educate people about privacy and data manipulation. An example here is "Game Time!," an app made by security consultant Aelon Porat. "Game Time!" is a pretext, much in the same way that Cambridge Analytica's "Sex Compass" was. Under the guise of providing a diversion to

the user, the "Game Time!" app gathered a tremendous amount of data about the user, from location to photographs to contact lists. However, unlike other apps, Porat's "Game Time!" also included a detailed and publicly visible log of the data collected. Porat uses that log to demonstrate to "Game Time!" players what those data could be used for: politically profiling the user, mapping their commute, and discerning their economic status based on their purchases.[20] All of this *comes from a game*. But, much like ethical social engineers, after Porat's app engages in trashing, pretexting, bullshitting, and penetrating, he drops the pretext to reveal the extent of the digital data his app collects.

So, in both the case of the ethical social engineers and privacy advocates like Porat, we may be manipulated, but very quickly they reveal their manipulations with the goal of opening our eyes to what social engineering can achieve.

And this is where the cases we have explored diverge. Masspersonal social engineering does not allow for pretexts to be dropped in time for targets to learn anything about manipulation. In the case of international conflicts, such as the Russian operation, there is, of course, never an intention to drop the pretext. Vladimir Putin repeatedly denies his government's involvement in the US election. At best, he claims again and again, private citizens were expressing their opinions online—nothing more.[21] At worst, Putin tells us, the masspersonal social engineering is an uncoordinated effort by individual "patriotic hackers."[22]

This is also true of Cambridge Analytica. To be fair, Cambridge Analytica employees did publicly present some of their tactics while they took a victory lap in 2017. People were justifiably curious as to how the company potentially helped elect a demagogue to office. However, even in the same presentations, they denied that the data they drew on were obtained unethically. When asked how Cambridge Analytica acquired their Facebook data, then-CEO Alexander Nix simply stated that any data that they had came

from people "voluntarily giving up their data. They're doing this in full knowledge of what's happening. This is nothing Machiavellian or untoward."[23] Such denials came at an ever increasing pace as more revelations about the company hit the news. Indeed, we would likely not know the extent of Cambridge Analytica's social engineering if it weren't for researchers like Emma Briant, reporters like Carole Cadwalladr, and whistleblowers like Brittany Kaiser and Christopher Wylie.

And even if Cambridge Analytica or Russia revealed the full extent of their masspersonal social engineering, whatever damage they managed to achieve was already done. The votes were cast and four years of Trump ensued. Contrast this with the limited scope of an ethical social engineering engagement.

Although their consequences are on a smaller scale, similar concerns can be expressed about "stealth marketing" campaigns. Consider a campaign in 2010, when attractive actors were paid by Blackberry to sit in bars and flirt with men, with the goal of getting the men to handle the new Blackberry Pearl phone and punch their phone numbers into it.[24] Mixing market research, pretexts, and bullshit, the marketing practice is clearly masspersonal social engineering. Soon, of course, such stealth marketing practices shifted online, with influencers being paid to surreptitiously (in the parlance of marketing, "natively") shill products they purport to believe in.[25] Even if these stealth marketing firms reveal their manipulation of consumers at a later date—perhaps in some celebratory article in *Ad Age*—the damage is done. The dollars are spent. Intense but one-sided personal relationships were forged. And even if the masspersonal social engineering is done out of putative desire to learn how social engineering works—as the Democratic operatives claimed they were merely doing during a senate race in Alabama—the end result will not be new knowledge, but increasing distrust in institutions and a warrant for masspersonal social engineering to be normalized as a legitimate method of strategic communication.[26]

So, we may be able to accept social engineering for ethical purposes in the limited case of hacker social engineers conducting penetration tests, or in the case of demonstrations of the extent of privacy violations happening online, so long as they protect the privacy and reputations of anyone they interact with, operate with integrity, and, most importantly, drop their pretexts and report their results in public *before* any damage is done due to their social engineering. Professionals like Conheady, Radcliffe, Hadnagy, and Porat do these things. Without these revelations, however, we see no possibility of the ethical application of masspersonal social engineering.

It is true that social engineers hired to do penetration tests do so on behalf of powerful clients—the corporate managers who hire them. The information they glean about how well employees secure information can be abused by those employers, who may choose to fire employees who are manipulated by the social engineers.[27] Moreover, the overall solution that ethical social engineers offer—we hack you so you can learn not to be hacked—relies upon a logic of individual responsibility for security, rather than considering security as a more social, organizational issue that large institutions should take charge of. These are flaws in ethical social engineering, but we think that they can be addressed without doing away with the entire field of ethical hacker social engineering.

What to Do about Masspersonal Social Engineering?

If masspersonal social engineering is predominantly unethical, and if it has the potential to undermine democratic debate (that is, if it hasn't yet already), we need to find ways to ameliorate the damage masspersonal social engineering does.

Masspersonal social engineering is not merely the problem of disinformation. Rather, it is enabled by a collection of difficult,

systemic challenges that span privacy and surveillance, cybersecurity, dark money in politics, the use and abuse of emerging ad tech, weak (or nonexistent) regulation of the influence industry, and more. Each of the elements of masspersonal social engineering relates directly to these more specific problems. Thus, we break down our suggestions based on each stage of masspersonal social engineering. Social engineering's reliance on these practices provides many avenues for mitigation. And even if masspersonal social engineering turns out to be ineffective, it's still worthwhile to consider solutions to problems like trashing, pretexting, bullshitting, and penetrating.

Trashing

The sheer lack of regulation of private data in the United States leads to gluts of information that enable trashing—or, to put it more politely, Big Data analysis—of unethically or illegally obtained personal information. Corporate social media sites are the main culprits here. But we cannot forget other, less well-known culprits: consumer profiling agencies like Acxiom, credit ratings firms, and governments, all of which collect as much data as possible under the assumption that, as communication scholar Mark Andrejevic puts it in his critique of unregulated data collection, "all data is potentially relevant no matter how seemingly trivial, irrelevant, personal, or invasive it may seem."[28]

It seems obvious to counsel people to avoid giving out their data—quit Facebook (and all of Facebook's subsidiaries) and Twitter, pay with cash, use a burner phone, use Signal, use Tor. Above all, we might point to frequent *Social-Engineer.org Podcast* guest Michael Bazzell's guides to becoming "digitally invisible."[29] As Andrejevic notes, "familiar norms of individual privacy threaten the data mining model to its core."[30] There are a host of personal privacy guides out there, and widespread adoption of their principles among individuals may in fact undermine trashing.

All of this seems fine until we think about how it puts an incredible burden on each of us to self-secure and take full responsibility for that security. Indeed, the advice to digitally disappear through the use of complex privacy tools and techniques like setting up shell companies in New Mexico echoes the advice given by professional hacker social engineers: it's up to *each of us* to secure *everything*. Be constantly aware of the information you share. In the extreme, trust no one.

Instead, we would argue for far better privacy laws and restrictions on how data are collected in the United States. Cambridge Analytica's Molly Schweickert implicitly acknowledges this solution in her post-mortem discussion of the 2016 Trump campaign. She presented her work in Germany, a country known for strong data protections, and her German audience was somewhat bewildered at the access to Americans' personal information Cambridge Analytica enjoyed. As she explained, the US relies on opting out of data collection. Every citizen must actively decline to have their personal data gathered. In contrast, Europe is opt-in.[31] This has not changed in the past several years—in fact, the 2020 Trump campaign was arguably even more invasive in its trashing practices than it was in 2016.[32] We suggest a key antidote to masspersonal social engineering can come in the form of making American companies adhere to far stricter data collection laws, with severe penalties for the sorts of abuses that Cambridge Analytica indulged in.

It is possible that the United States will catch up to the European Union in this regard and thus alleviate masspersonal social engineering. The March 2020 report from the US Congress's Cyberspace Solarium Commission explicitly connects the insecurity of personal data to the rise of social engineering. The report predicts that

> Authoritarian states will take advantage of preferred relationships with technology firms to build in backdoors for government access that allow them to surveil the private lives of citizens and political opponents at home and abroad. In addition to advertising,

> propaganda will be micro-targeted and tailored to an individual based on personal data and search history.[33]

With such surveillance capacities in place,

> The information stolen from American entrepreneurs, public officials, industry leaders, everyday citizens, and even clandestine operatives is fueling social engineering and espionage campaigns against US firms and agencies.[34]

Due to increasing capacities for targeted propaganda and social engineering—that is, masspersonal social engineering—the report calls on the United States Congress to "pass a national data security and privacy protection law establishing and standardizing requirements for the collection, retention, and sharing of user data."[35] We concur, so long as the legislation includes directives to make the collection of personal information opt-in.[36]

One possible side effect of increased regulation of data-mining corporations may be less waste. As we have argued, trashing relies on a political economy of waste, where waste is a forgotten byproduct of consumerism. Likewise, surveillance capitalism relies in large part on our forgetting about our data. Just as the trash is picked up from the curb and taken . . . *somewhere* (do you know where your local dump is located?), so, too, do the data collection practices of corporate social media, app developers, and device software makers take our data *somewhere*. It's 2022. Do you know where your data are? Do you know where the nearest Google or Facebook data center is located? Perhaps you don't, but know this: it is massive, it consumes a great deal of energy and water, and it is not going to shrink or disappear so long as our personal data are easily obtained.[37]

Even if we severely curtail the future collection of personal data via legislation, there is still a great deal that has already been collected. We cannot forget this. To combat the data/trash/forgetting triad, we need a radically different relationship to the flows of information. Just as we need to grapple with the mounds of waste we are

generating, we will have to grapple with the materiality of information as data are stored in massive server farms. As environmentalist and media studies scholar Mél Hogan argues in her criticism of data collection,

> While we equip ourselves with mass surveillance capabilities and are complicit in continuously generating data, we are not cognizant of the fact that our tracked bodies exist within a material world: one that is slowly compromised at the expense of being watched, detailed, and archived, in bits and numbers.[38]

In addition to an opt-in culture of personal data collection, there should be limits on how long the data are retained. And this means that the corporations who have gathered our data need to be required to delete our personal information rather than indefinitely store it—unless we affirmatively opt in to having a permanent record.

Pretexting

Role-playing, in itself, is not necessarily a problem. There are many instances in which people may want to play roles. A common example is the identity play that happens online. Such roles allow people to explore aspects of themselves that might in other contexts put them at risk. The cases where pretexts are used to harm other people—as in the case of interpersonal con artistry—are cases of fraud, plain and simple, and can be prosecuted as such. Otherwise, there is no pressing need to eliminate role-playing.

But the glut of "dark money" flooding politics—thanks in part to the US Supreme Court's 2010 *Citizens United v. FEC* decision—allows for well-funded pretexts on a national scale. Dark money "is money that has been routed through an opaque non-profit—thus concealing its true source from voters and investors alike."[39] This is, of course, a pretext straight out of the old mass social engineering playbook. Just as Edward Bernays, Doris Fleischman, and Ivy Lee might have created front groups to advocate positions on behalf of

their clients, today's super PACs are advocating political positions for their wealthy and untraceable donors.[40] The explosion of dark money-funded groups can fundamentally shift politics away from the political parties and towards "'shadow parties'—organizations outside of the party that house the party elites."[41] These shadow parties will be beholden only to their unknown donors and can shape political programs by simply choosing which politicians get the money they need to campaign.

Compounding this is the eagerness for corporate social media to sell advertising space to anyone willing to pay for it. To rectify these problems, corporate social media sites may want to eradicate political advertising altogether if they cannot control who is buying the ads—particularly when the purchasers are coming from outside the state holding an election. But the temptation to get a slice of the now billions spent on electioneering is likely too great. Facebook argues that its "ad library" provides transparency in terms of political ad spending, but researchers have found that Facebook's attempt at self-regulation is woefully inadequate, rife with inconsistencies and missing information.[42] This allows for ads produced through pretexts to continue to flourish.

It's not just Facebook's self-regulation that is inadequate. Past mass social engineers have tried self-regulation and it simply does not work. The use of pretexts known as "front groups" has been discouraged by the Public Relations Society of America Volunteer Chapter since at least the 1950s because such pretexts create the false impression of popular support for positions held by powerful corporations and governments.[43] However, because public relations is a self-regulating industry, there are no effective ways to prevent public relations firms from setting up the same sorts of front groups Bernays and Fleischman were famous for. The use of front groups is only increasing as super PACs gain power and corporate social media seeks to sell access to their audiences. In the case of elections, since they in particular are fundamental public goods, then

it follows that they should be publicly funded, full stop, with no private money being used to fund campaigns.[44]

Bullshitting

Perhaps the most difficult social engineering element to combat is bullshit. There is, simply put, a great deal of truth-indifferent communication that mixes deception, accuracy, and friendliness. From the moment we wake up and see our first advertisements on our phone until we fall asleep thinking about the day's political, economic, and cultural news, we will confront an overwhelming stream of bullshit. This is not to mention daily conversations with coworkers, friends, family, and strangers, all of which might contain elements of deception, accuracy, and friendliness.

The bullshit we encounter among friends, family, and co-workers may not have a true antidote, other than our occasionally calling it out. Recall Chandra Mukerji's study of the hitchhikers, which argues that bullshit is often about maintaining social bonds.[45] The social penalty for calling out our loved ones' bullshit might include estrangement from them. Holiday gatherings will probably be even more awkward.

Mediated bullshit, however, has an ancient adversary: media literacy. For every production of mediated bullshit, from advertising to public relations to contemporary disinformation campaigns, a host of scholars and activists leap up in challenge. The lessons provided by the Media Education Foundation in the 1990s are carried on by the work of the scholars at the Data & Society think tank and the Technology and Social Change Research Project at Harvard. The latter has given us the Media Manipulation Casebook, an excellent resource for decoding online misinformation campaigns.[46]

A notable example of anti-bullshit media literacy work is the #YourSlipIsShowing hashtag movement of Black feminists. Unlike the more formal projects, #YourSlipIsShowing is more of an ad-hoc effort, but one that exposed many of the same sorts of pretexts the

Russians and others would go on to use. In a remarkable feat of internet research, these Black feminists traced fake Twitter accounts, which purported to be the accounts of Black activists, to their 4chan progenitors, who turned out to be racists, men's rights activists, and pickup artists. However, despite the important work of #YourSlipIsShowing, this movement has largely gone unsung: "one of the earliest crowdsourced anti-misinformation campaigns on the internet has been mostly ignored by the mainstream media."[47]

In addition to dissecting mediated bullshit as the #YourSlipIsShowing activists did, we must also question the systems in which it thrives. We have to ask critical questions as to why this bullshit is before us and why it displaces other, non-bullshit messages.[48] As media literacy scholars have argued since at least the 1990s,

> The goals of a loosely regulated, commercial media have no educational, cultural, or informational imperatives. As much of the literature on the political economy of the media suggests, they are there to maximize profits and to serve a set of corporate interests.[49]

We should consider media as systems, not as loose collections of texts. This perspective orients us to what we might call the political economy of bullshit.

Knowing the economics of bullshit takes on a new urgency in these days of masspersonal digital media, where text is increasingly customized for each individual and where conspiracy theories and misinformation reign supreme—and where the sources of such messages might be obfuscated. As one contemporary guide to media literacy argues, "it is necessary to rethink media literacy in the age of platforms."[50] While we undoubtedly agree, rethinking media literacy needs to go further. Social media platforms are a big part of the problem, but as we have argued in this book, masspersonal social engineering implicates even greater systemic problems at the intersections of technology and politics. Media literacy in the age of masspersonal social engineering requires literacy about the problems that allow for trashing, pretexting, and penetrating, too.

Media literacy to combat masspersonal social engineering is not just about media but also about privacy, surveillance, cybersecurity, and more. And, it also requires us to take back ownership of social media, perhaps in the form of community-owned, non-profit social media systems.[51]

This brings us back to the sort of bullshit we might get from friends, family, and co-workers. This sociable bullshit takes on newer, potentially damaging forms when it is channeled through corporate social media. It shifts from relatively harmless, interpersonal discussions to masspersonal media—especially because Facebook and other corporate social media are built to amplify messages our contacts share with us.[52] Our relatives become vehicles for bullshit and hence possible vectors for masspersonal social engineering. Tackling mediated bullshit—especially as it appears on corporate social media, as contemporary media literacy advocates urge us to do—may help us address local, familial bullshit.

Penetrating

Of course, the most obvious penetration-related problem we face is the woeful state of cybersecurity among public and private institutions in the United States. While US cybersecurity discourse for years focused on the potential for catastrophic cyber doom scenarios leading to physical destruction and loss of life, the events of 2016 and later—including recent massive hacks of corporate and government networks as part of the 2021 SolarWinds incident—have driven home the message that the dominant cyber threats are informational. Cybersecurity is threatened by espionage, intellectual property theft, and the over-collection and misuse of personal data.[53] That is, it is threatened by trashing. But in addition to the trashing-related suggestions mentioned above, we can mitigate such threats by, in essence, doing a better job of locking the doors, preventing systems that hold such data from being penetrated in the first place. Once again, we suggest taking seriously the many

proposals found in the recent Cyberspace Solarium Commission Report in this regard.[54]

But the penetration metaphor has many fathers, including schools of communication that have produced generations of people who conceive of communication as a game of penetration. As the former Cambridge Analytica employee turned whistleblower Christopher Wylie put it, from this perspective,

> culture change can be thought of as nudging the distribution curve of culture up or down. What the data allowed us to do was to disaggregate that culture into individuals, who became movable units of that society.[55]

This view of culture emerging as the sum of communicative nudges of individuals is precisely what historian of communication Christopher Simpson called the "science of coercion," or "communication as domination."[56] More polite terms include "strategic communication" or "media effects," where carefully calibrated messages can master crowds or shape individuals' opinions. Such thinking leads directly to the epistemology of masspersonal social engineering, which would elevate the penetrating effects of communication over all other considerations. Although he's talking about seducing women by any means possible, the pickup artist Ross Jeffries summarizes this view quite well: "the purpose of your communication is not to give her an understanding. The purpose of your communication is to get you a result!"[57] Add up all these "results," this line of thinking goes, and a social order emerges.

Moreover, this communication-as-penetration model slips easily into the mouths of people who would characterize all communication as a military endeavor. While this book is deeply indebted to security researchers, we find that too often the language they reach for is militarized and securitized. Just as we have offered an explanation of the process of masspersonal social engineering, there have been several other attempts in recent years to describe the stages of information operations, fake news, disinformation, social media

manipulation, and malignant foreign influence campaigns.[58] For example, security analyst Bruce Schneier takes up defense contractor Lockheed Martin's concept of the "cyber kill chain" to theorize the cycle of information operations. In drawing on researchers like Schneir and offering our own process, we appear to be offering a "cybersecurity kill chain" of our own. However, we would reject this characterization. This kind of language is a result of a narrow vision of how to talk about what we're calling social engineering. The conceptual universe of "cyber" has been so thoroughly militarized that, as soon as something is framed as cybersecurity, everything about it—from diagnosis to solution—becomes a military problem. The penetration metaphor of communication—where messages are bullets—has become the dominant language for talking about all things cyber, including disinformation.[59]

This approach has, of course, been criticized for generations. Communication theorist James Carey famously called it the "transmission model" of communication.[60] Christopher Simpson's "science of coercion" is a harsher condemnation. They join cultural studies scholar Raymond Williams, who noted in the 1960s that

> it is indeed monstrous that human advances in psychology, sociology, and communication should be used or thought of as powerful techniques *against* people, just as it is rotten to try to reduce the faculty of human choice to 'sales resistance'. . . . Much of this talk of weapons and impact is the jejune bravado of deeply confused men [sic].[61]

Our contribution to this critique is modest: we simply want to join the ranks of all those who maintain communication is richer and more than the penetration metaphors of penises and bullets would have us believe. Against these penetrating metaphors, we turn to colleagues who repeatedly envision a better model of communication.

Instead of communication as penetration, we agree with communication scholar Guobin Yang's argument for "communication

as translation." Drawing on insights from a range of thinkers, including Williams, Carey, Walter Benjamin, and Patricia Hill Collins, Yang argues communication-as-translation "is premised on the recognition of difference, dialogue, receptivity, mutual change, and self-transformation."[62] Like translation across languages, communication as translation is a series of utterances that are bounded in meaning (they relate back to the original language or statement), but at the same time, they are boundless in interpretation. We are constantly translating one another—even if we speak the same language. Moreover, as Yang argues, if we acknowledge communication as an act of translation, we ought to be open and listen to people who do not share our backgrounds, most especially people whose voices are not often translated to the mainstream.

Yang's approach echoes Black feminist scholar Patricia Hill Collins's call for dialogue and coalition-building across autonomous groups.[63] Collins uses the concept of a multiplicity of stories to elaborate on this approach, noting how storytellers are "writing one immense story, with different parts of the story coming from a multitude of different perspectives."[64] The gathering up of such narratives could "form constellations illuminating experiential particularity," a "democratic communication that is inclusive without suppressing particularity."[65] In this vision, the "universal become[s] a fluid and emergent terrain of agreement, a space for becoming in difference."[66] This is opposed to a predetermined universal being imposed upon the multiplicity of people's stories—the eradication of difference, a Big Translation of all ideas into one dominant story.

As tempting as it might sound, this vision of emergent, from-below storytelling, dialogue, and coalition-building is decidedly not data-driven. Particular stories are not data points to be aggregated into a Big Dataset that can allow for analysis without theory. Rather, the narratives that are being produced are coming from autonomous groups—including and especially marginalized groups—who

are defining themselves and then actively articulating their views with other groups. We echo Collins's warning that autonomous groups, such as Black feminists, must define themselves and not be defined by others:

> Because self-definition is key to individual and group empowerment, ceding the power of self-definition to other groups, no matter how well-meaning or supportive of Black women they may be, in essence replicates existing power hierarchies. . . . As Audre Lorde points out, "it is axiomatic that if we do not define ourselves for ourselves, we will be defined by others—for their use and our detriment."[67]

Moreover, narratives are not things to be controlled, penetrated, or dominated. Narratives are collective, locally negotiated and defined, and then translated into new contexts, bearing with them traces of their previous meanings while being open to new meanings.

Yang's communication-as-translation, then, is not about dialogue across differences theorized by those who—including the adherents of the communication-as-penetration model—would sort people into specific types and use such typologies to craft messages to manipulate them. Rather, it is about the "complex unity in difference" that emerges as such autonomous groups build coalitions through dialogue.[68] Such complex unity has space for the social engineers, perhaps, but it does not endorse their limited vision of communication as penetration.

To put this another way, we do not share the faith of those who want to use "data for good." Even the critics of Cambridge Analytica, the whistleblowers Brittany Kaiser and Christopher Wylie, hold onto the view that enough data in the hands of good elites can lead to social and economic justice.[69] Kaiser's own eagerness to search for "data for good" led her to praise Phunware in the pages of her book, calling it "a Big Data company that is returning the data they hold to consumers and rewarding them for its use."[70] Phunware would go on to make the Trump 2020 campaign app, by some measures one

of the most invasive apps ever used in US politics.[71] This desire to use communication as penetration for good echoes the views of the mass social engineers, who arose during the early twentieth century and held that scientific "facts" (presented in the right way) could be used to implement a perfected society. The parallels between the social reformers of the early twentieth century and progressive data scientists of the early twenty-first century are startling: they all start with an earnest belief that data can inform social justice, but they gravitate towards people in power in the blind belief that at best those powerful actors will support their data- or fact-driven social justice goals, or at worst they can take the money they earn from their penetration campaigns and someday use it for good. No matter their desire to do good—through health campaigns, or public service campaigns, etc.—the penetrative communication approach is readily appropriated by those in power.

When those in power inevitably use data and communication to maintain and strengthen social hierarchies and inequalities, we act surprised. We should not be. And this leads us to a critique of those who take a more critical approach to communication, as we do. If the communication-as-domination view places too much emphasis on effects, critical scholars have often placed too little emphasis on thinking more expansively about the effects of communication. Clearly, communication, whether mass, interpersonal, or masspersonal, has effects. But we need to think more about effects as broader than just the linear penetration of individual minds and the changing of individual behavior (e.g., political opinion and voting) to consider communication effects as nonlinear and emergent phenomena that exist and are important, but that may not be amenable to the quantitative social science methodologies that predominate in traditional media effects research. Thus, we support recent efforts by communication scholars to take a more critical approach to the study of strategic communication, as well as to create a "critical media effects framework."[72]

Again, however, let us repeat that each of these practices—trashing, pretexting, bullshitting, and penetrating—are not in themselves masspersonal social engineering. Their concatenation is the problem. We are wary of anyone who trashes us. We are wary of anyone who uses a pretext. We are most definitely wary of people who bullshit us. And we are wary of people who seek to penetrate us. But we should be most concerned about the masspersonal social engineers who put all of these practices together into a new form of manipulative communication.

Fortunately, any chain can be broken at any given link. What we offer here is, admittedly, only a start to how we might do that. We invite others to help further our understanding and options for breaking the chain of malicious use of masspersonal social engineering.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Gehl, Robert W., author. | Lawson, Sean T., 1977–author.
Title: Social engineering : how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication / Robert W. Gehl and Sean T. Lawson.
Description: Cambridge : The MIT Press, 2022. | Includes bibliographical references and index.
Identifiers: LCCN 2021016750 | ISBN 9780262543453 (paperback)
Subjects: LCSH: Social media—Security measures. | Computer networks—Security measures. | Internet fraud. | Social engineering.
Classification: LCC HM742 .G45 2022 | DDC 364.16/3—dc23
LC record available at https://lccn.loc.gov/2021016750

10 9 8 7 6 5 4 3 2 1