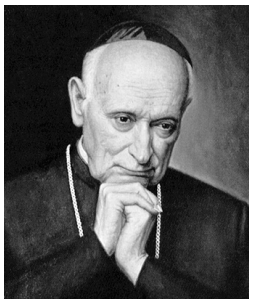
Mindszenty Report



June 2019 Cardinal Mindszenty Foundation Vol. LXI-No. 6

Social Media in the Information Age

Big Data Collection Brings Benefits But Allows Manipulation

Try looking up in Google Books *The Autobiography of Margaret Sanger*, in which she discusses speaking to women of the Klu Klux Klan in 1926 about birth control. You will discover that a chapter is missing in which she describes how the Klan welcomed her message on the need for birth control to limit growth of the black population. Google Books blocks this chapter from viewing. What this reveals is how a corporation can control and manipulate public information.

This control of information is apparent in Google's search engines and news feeds. Researchers at Northwestern University recently examined how Google algorithms worked in search results for news-related queries. They collected 6,302 unique links to news articles shown in the Top Stories box. The top sources were the left-wing CNN, the *New York Times*, the *Washington Post*, *The Guardian*, the *Los Angeles Times* and *Politico*. CNN led the list with nearly 11 percent of the links. Fox News came in at only 3 percent of the links. Of user-sharing links on Facebook, 62.4 percent of the articles came from news sites rated by the research team as left-leaning, whereas a little over 10 percent came from sources considered right-leaning.[1]

Facebook controls news in other ways. When parliamentary elections for the European Union approached in late May, Facebook monitored misinformation, fake accounts and election interference that violated the site's rules. This monitoring was similar to what Facebook constructed to monitor the U.S. midterm elections in 2018. In this case, the monitoring focused on multiple countries.

Facebook staffed its monitoring team with 40 people, including native speakers of all 24 official EU languages. Monitors look for material that is flagged by automated systems or by users, and after a team review, a recommendation is made as to whether the posts (or bulk posts) should be removed. Although Facebook executives claim that their efforts are designed to ensure fair elections by preventing fake news or foreign interventions, critics asserted that Facebook interventions targeted Euro-skeptics.

In early May, Facebook took down 23 Italian accounts with a total of more than 2.6 million followers for spreading "false information and divisive content" over issues such as migration, vaccines and anti-Semitism. More than half of those Italian accounts were supportive of either the 5-Star Party or the League, the two parties that constitute the coalition government in power today.[2]

We know that Google, Facebook, Amazon and their spinoff companies collect huge amounts of data which is sold to commercial interests for marketing. Political campaigns use this mega-data as well for micro-targeting voters. Those who did not grow up with social media might worry that a corporation knows about one's age, gender, marital status, family members, television programs watched, books read, clothes purchased, home residents and price, and an aerial shot of the house and neighborhood. Members of the younger generation might joke occasionally about what big corporations know about them, but nonetheless they are generally willing to reveal exceedingly intimate details about themselves. "Sexting" is not rare among the young.

Shaping Behavior

Yet the larger question is what these corporations are doing with the massive amounts of information they collect on individuals. Their goal is not just to collect and sell data. They also hope to shape consumer and voter behavior into recognizable, predictable patterns.

Three important questions are raised by this new technology: What is the meaning of privacy in this age of aggregate information collection; how can this mega-data be used politically; and can corporations (and government) shape individual behavior through social media?

Personal data is gold to big media corporations. Even the most mundane things an internet user does are translated

into mega-data to be analyzed through complex algorithms. Watching a movie, ordering a book or clothes, posting a photo of a puppy, Google searches—all become data points. All this data is collected through implicit consent of the user. Consent is often given through buried "terms of service" agreements.

Internet and smartphone users know that corporations are collecting data. What many don't know is how the data is used for other purposes. For example, when a person sends in material for a DNA test to trace their ancestry, this person might not know that the genomic company doing the testing will resell your data to pharmaceutical firms. A hedge fund might buy your location data to analyze stores you frequent.[3]

Amassing data is legal. Some states have tried to place restrictions on data brokers, but generally the industry is unregulated. There is no regulatory agency overseeing how social media collects and shares data. The courts are just beginning to explore privacy issues and mega-data collection. Most people agree that much of the information shared on the internet is benign and contributes to a global storehouse of knowledge. The internet creates convenience for its users. Using Google Maps and getting voice travel directions is better than having a large, cumbersome map on the car seat next to you.

Nevertheless, each day users around the globe upload billions of photos, videos, text posts and audio clips to YouTube, Facebook, Instagram and Twitter that are fed into computers to be translated into algorithms. Facebook, Google and other companies use "cookies"—pieces of code set into the browser—that allow users to be tracked as they surf the web. Furthermore, Google (among other companies) in 2016 revised its privacy policy to permit personally identifiable web tracking to merge browsing data with personal information collected from services such as Gmail. The consequence is that Google and Facebook can target ads based on your name.

New Tools for Solving Crimes

The next frontier in data collection—and it is already here—is data gathered from facial recognition. Facial-recognition technology has some very positive uses, notably in law enforcement. Shockingly, the city of San Francisco passed an ordinance on May 15 forbidding the use of facial-recognition technology by police and other government departments.

Yet mega-data collection raises real issues of privacy. Do we want health insurance companies to have access to messaging on Instagram posts? Should colleges be allowed to monitor posts of teenage applicants?[4] Some have argued that stricter privacy laws need to be enacted, but one of the big problems is that we do not know all the ways that information is being collected, sold or traded. Furthermore, the rapidity of technological advances in data collecting, analysis and use makes it difficult for legislators to enact laws that protect individual privacy.

What has developed in the United States is surveillance capitalism—the monitoring of all possible data that can be acquired about us.[5] Google Home can recognize voices and routines. Amazon's Alexis listens to conversations and knows what we need. Google Photos knows faces of friends, as well as where they are traveling by their posts. YouTube follows what we watch and who watches, accumulating information about the user's interests. Google Maps tracks where we are through our phones. DNA is being collected.

'Forensic Genealogy' Catches Killers

FamilyTreeDNA advertises that by submitting one's DNA to the company, a person can help catch a criminal. This has real benefits, as became evident when police in California arrested the alleged Golden State Killer, a criminal who murdered at least 13 people and raped at least 50 women. The Golden State Killer was tracked down by using DNA data from the company. Subsequently, dozens more arrests were made of rapists and murders using these same techniques.[6]

FamilyTreeDNA came under fire when it was revealed that the company was quietly working with the Federal Bureau of Investigation. The company's website allows people to upload to its website genetic profiles from competitors including 23andMe and AncestryDNA. In late 2018, FamilyTreeDNA changed its terms of service to allow investigators to upload a suspect's DNA profile to find potential relatives. FamilyTreeDNA allows U.S. customers to opt out of law enforcement matching, but only 1 percent of U.S. customers appear to have opted out.

Surveys show that the majority of Americans support what is called forensic genealogy.[7] Although not all American jurisdictions have adopted it, forensic genealogy is a great boon to law enforcement and should be utilized wherever possible, at least for investigations of violent crimes. The District of Columbia and Maryland have laws banning certain kinds of forensic genealogy. California, Colorado, Texas and Virginia require law enforcement to exhaust all other avenues first before resorting to genealogy database searches leading to familial DNA matches.

At the end of April Facebook revealed its new design for its website and mobile app, the first major redesign since the social network was launched in 2004. The new website encourages users to reveal even more personal beliefs and

details about their lives.[8] The redesign urges users to join groups. According to Facebook, even before the new design 400 million of the company's 2.37 billion active users were participating in group chats. This push for group users raised concerns from privacy advocates. Adam Levin, founder of the Scottsdale, AZ-based CyberScout, a global data and identity protection company, warned, "By creating groups we will be doing Facebook's work for it. The more people who come together to talk about their interests—whether they're political, financial, or religious—the more data Facebook can collect. There's nothing more delicious for Facebook than having people come into groups and talk."[9]

Other critics warn about the intrusion of social media into our private lives. In particular, critics warn of the "living room" concept of surveillance. Karen Kovacs North, a communications professor at University of Southern California, said, "We forget that the company that's hosting our conversation is also listening. ...Anything you think is private is public, and anything you think is temporary is permanent. Facebook aggregates data for advertisers, but other people can simply take a screenshot."[10] In this way, the private becomes public, and the private becomes aggregated for micro-targeting.

The Personal is Political

Political campaigns use aggregated data to micro-target voters. As a registered voter surfs the web, a tiny piece of data, a cookie, flags your political preferences. The cookie allows information to be gathered as to party affiliation, political contributions, and possibly estimated income, occupation and recent purchases. The firm Campaign Grid compiled the following information on one internet user: "Lives in Pennsylvania's 13th Congressional District, 19002 zip code, registered primary voting Republican, High net worth household. Age 50-54. Teenagers in home, Technology profession, Interested in politics, Shopping for car, Planning a vacation in Puerto Rico."

Campaign Grid later withdrew this information from its website, but its collection of data, which is sold to campaigns, is impressive. Campaign Grid collects 18 different attributes for every voter. This data is sold to campaigns for online ads targeted to the individual voters. Campaign Grid is only one of seven companies in the business of selling data. Campaign Grid primarily works with Republicans, while Precision Network works with Democrats. Precision Network has a larger collection of data, with political information on 150 million American internet users, or about 80 percent of the nation's registered voters.[11]

Yahoo, Google and Microsoft sell access to their political data to candidates. Democrats entered aggregated data collection early, leaving Republicans to play catch-up. In 2008, Barack Obama's presidential campaign launched a data operation which assigned every voter in the United States a pair of scores predicting how likely it was for them to cast a ballot and predicting whether they would support him.

Consultant Ken Strasma boasted in 2012 that the Obama campaign knew whom "people were going to vote for before they decided."[12] By 2016, political campaigns were harvesting huge amounts of data that transformed how candidates mobilized and communicated with voters. As more people received their news from social media, political campaigns micro-targeted votes through online ads, personalized phone calls and voter canvassing.

Social Media and Behavior Modification

Political campaigns—and social media—have undertaken extensive research into psychology. Corporate social media companies are in the business of selling data, so the more information they can collect, the higher their profits. But these corporations want more than just information. Their goal is to change behavior through social media.

Shoshana Zuboff in her new book *The Age of Surveillance Capitalism: The Fight for a Human Future at the Frontier of Power* (2019) details at great length the stated goals of social media corporations to adjust user behavior. Zuboff is on the left politically. Her book is long and repetitive but revealing. Her concerns should be shared by the left and the right. She reveals the extent and rapid advance of surveillance technology and the heavy investment social media corporations have made in individual psychology in order to affect behavior.

An example she points to of the advancement of surveillance technology is the "smart-home." One device of the new "smart-home" is Google's Nest-thermostat. It uses motion sensors and computation to learn the behaviors of a home's inhabitants. Nest's apps can gather information from other connected products such as cars, ovens, fitness trackers and beds. It can send notifications not just to homeowners but also to insurance companies, physicians, advertisers and other third parties.

Through the collection of such data, social media corporations want not only to automate information flows, but to "automate us." For example, an insurance company will be able to monitor driving, from "fastening the seat belt to rate of speed, idling times, braking and coring, aggressive acceleration, harsh braking, excessive hours on the road, driving out of state, and entering a restricted area." Researchers anticipate the fusion of "smart cities" with "smart health."

The mapping of human emotions for the marketing and advertising sector and the political arena is projected to reach a $53 billion industry within the next few years. Facebook and Google have invested heavily in studies on how to change behavior. Google and Facebook are learning to discern user "activities, interests, mood, gaze, clothing, gait, hair, body type, and posture." Machines can capture in a nano-second signs of disgust that precede anger, comprehension and joy. As early as 2014, Facebook had applied for an "emotion detection" app patent. Detecting immediate emotions increases the probability of certain outcomes.

Alex Pentland, director of the Massachusetts Institute of Technology's Human Dynamics Lab, is a guru in the field. He envisions a collective society that provides social awards for "efficiency." Pentland declares, "For society, the hope is that we can use this new in-depth understanding of individual behavior to increase the efficiency of industries and governments." For the individual this is a world of convenience where everything is arranged, from your health check-up, to driving, to ordering food. He concludes that as our "abilities become refined by the use of more sophisticated statistical models and sensor capacities, we could well see the creation of a quantitative, predictive science of human organizations and human society."[13]

This new technology offers convenience to consumers, safety to the public, and efficiency to politicians and corporations. What is threatened are privacy and free will. Individuals are free to take steps to limit the amount of personal information they place online, but such steps require vigilance. (The task could get easier: in late May Senator Josh Hawley (R-MO) introduced a bill to give Americans the ability to join a "Do Not Track" list with a single click in their browser's settings.) Privacy-loving individuals must to some extent limit their usage of popular (and effectively monopolistic) social media services. Moreover, a considerable amount of personal information is considered public and may not be protectable from data collectors, such as homeowner addresses, voter registrations, voter participation, campaign donations, and involvement in court proceedings.

The founders of our Constitution valued, perhaps above all else, private individual rights. Our Catholic faith is founded on the principle of free will. The new world envisioned by corporate promoters of the age of surveillance undermines both principles—privacy and freedom of choice. Totalitarian communist and fascist states seek to control and manipulate behavior. Today, social media corporations, on a road paved with good intentions, seek a new sort of collectivism. It remains to be seen whether the gains will outweigh the losses to a free society. Fasten your seat belts.

1 John Sexton, "Audit: Google Favors a Small Number of Left-Leaning News Outlets," *Hot Air*, May 10, 2019.
2 Andrew Liptak, "Facebook Set Up a War Room to Combat Misinformation Ahead of Europe's Parliamentary Elections," *The Verge*, May 5, 2019; and "Facebook Takes Down Fake Italian Accounts Ahead of EU Election," *Reuters*, May 5, 2019.
3 Louis Matsakis, "The Wired Guide to Your Personal Data (and Who is Using It)," *Wired*, February 15, 2019.
4 Ibid.
5 Jason Evangelho, "Why You Should Ditch Google Search and Use DuckDuckGo," *Forbes*, October 3, 2018.
6 Sarah Zhang, "A DNA Company Wants You to Help Catch Criminals," *The Atlantic*, March 29, 2019.
7 Ibid.
8 Quentin Fottrell, "Mark Zuckerberg Wants People to Join Facebook Groups, But Critics Say It's Another Way to Collect Your Most Intimate Data," *Marketwatch*, May 5, 2019.
9 Ibid.
10 Ibid.
11 Lois Beckett, "How Companies Have Assembled Political Profiles for Millions of Internet Users," *ProPublica*, October 1, 2012.
12 "Case Study: Profiling and Elections—How Political Campaigns Know Our Deepest Secrets," https://privacyinternational.org/case-studies/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets.
13 Quoted in Shoshana Zuboff, *The Age of Surveillance Capitalism*, p. 429.

Mindszenty Report Reprints

THE MYTH OF THE INCARCERATED NATION. The movement to reduce U.S. incarceration scored a victory with the First Step Act signed by President Trump, but caution is in order before allowing large numbers of violent criminals to go free. Recidivism rates are appalling, and no one should want to reverse the success of the system in reducing the high crime rates of a generation ago. Ask for 5/19

ENGINEERING THE NEW HUMAN. A Chinese scientist's unsettling experiment in altering the genes of twin girl embryos, who have since been born, has caused soul-searching in the international genetic research community. Ask for 4/19

The Mindszenty Report is published monthly by

Cardinal Mindszenty Foundation
7800 Bonhomme Ave.
St. Louis, MO 63105
Phone 314-727-6279 Fax 314-727-5897

Subscription rate: $25 per year
Outside the U.S.A. $35

Contributions to the Cardinal Mindszenty Foundation are tax-deductible to the extent allowed by law.

web site: www.mindszenty.org
orders.inquiries@mindszenty.org