Big Brother Goes into Business

MARTIN WITKERK

Shoshana Zuboff is a Harvard-educated social psychologist whose work has focused on technology in the modern corporation. In this important new book, she describes a fundamental shift in our economic order: the prediction and influencing of human behavior, enabled by constant surveillance with computing devices. Google was the original pioneer of this new form of capitalism, and Facebook and Microsoft soon joined in. Now we are witnessing a generalized scramble toward maximizing data capture and converting it into corporate revenue. Corporations' assurances that they "value their customers' privacy" have done nothing to slow down the revolution.

Google was founded in 1998, two years after the Mosaic browser opened the World Wide Web to computer users. By the time the young company held its first press conference in 1999, they were already fielding seven million search queries every day. Yet they do not seem to have begun with any clear business model. The founders understood that the ability to search the metastasizing and ever-changing Internet would soon become a critical ability, and therefore worth plenty of money. The venture capitalists who initially supported Google obviously agreed. But it was not clear at first *who* was actually going to pay for Google's services: their basic search function was always free to the individual user, as it remains today. The answer was to come from an unexpected quarter.

Every Google search produces a great deal of data: not only key words, but "the number and pattern of search terms, spelling, punctuation, dwell times, click patterns, and location." In the company's early days, these accidental byproducts of Internet searching, referred to as "data exhaust," were "haphazardly stored and operationally ignored." A young Stanford graduate student named Amit Patel studied Google's accidental data logs and arrived at the conviction that

> detailed stories about each user—thoughts, feelings, interests—could be constructed from the wake of unstructured signals that trailed every online action. Google's engineers soon grasped that the continuous flows of collateral behavioral data could turn the search engine into a recursive learning system that constantly improved search results and spurred product innovations such as spell check, translation, and voice recognition.

All of this improved search results, but still did not provide the company with any "reliable way to turn investors' money into revenue." In those early days, the company's income "depended on exclusive licensing deals to provide web services to portals such as Yahoo!"

THE AGE OF SURVEILLANCE CAPITALISM

The Fight for a Human Future at the New Frontier of Power
By Shoshana Zuboff
New York: Public Affairs, 2019
692 pp., $38.00 hardcover

Competing search engines charged commercial websites a modest fee for indexing them, but Google never went this route. Nor was advertising initially central to the company's plans. Cofounder Larry Page had even expressed concern that "advertising funded search engines will be inherently biased toward the advertisers and away from the needs of the consumers." Google's AdWords team consisted of just seven employees who generated a modest revenue from sponsored ads linked to search query key words.

In the spring of 2000, the dot-com bubble burst, and investors' willingness to throw money at new technology in the vague hope that something would eventually come of it suddenly dried up. Google was under pressure to show investors real returns, and the company "tasked the tiny AdWords team with looking for

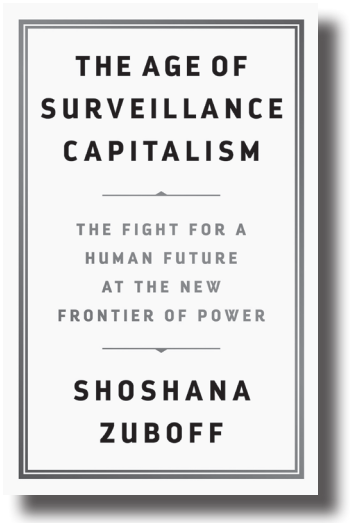
Martin Witkerk *writes from the mid-Atlantic region and has a Ph.D. in philosophy from Tulane University.*

ways to make more money."

Before Google got into the business,

> advertising had always been a guessing game: art relationships, conventional wisdom, standard practice, but never "science." The idea of being able to deliver a particular message to a particular person at just the right moment when it might have a high probability of actually influencing his behavior was the holy grail of advertising.

Google's AdWords team, however, realized this ideal could be brought closer by exploiting their enormous cache of collateral behavioral data. The author christens behavioral data available for uses other than service improvement *behavioral surplus*. The repurposing of Google's data caches from improving user services to increasing returns on advertising amounted to *the birth of surveillance capitalism*, based on the accumulation of behavioral surplus.



New data sets known as "user profile information" were compiled to enhance the accuracy with which future behavior (both ad views and actual purchases) could be predicted. And there was no reason why *all* this personal information needed to come from Google's own caches:

> Some elements of [online] surveillance had been operational for years. For example, the software mechanism known as the "cookie" — bits of code that allow information to be passed between a server and a client computer — was developed in 1994 at Netscape, the first commercial browser company. Similarly, "web bugs" — tiny (often invisible) graphics embedded in web pages and e-mail and designed to monitor user activity and collect personal information — were well-known to experts in the late 1990s.

By means of such mechanisms, user data could be hunted down anywhere in the online world. A user's profile information might include other pages he had visited, advertisements he had viewed there, and purchases he had made. The new data "meant there would be no more guesswork and far less waste in the advertising budget." Google targeted its ads to individual users, tracked how often users actually clicked on an ad (known as the "click-through rate"), and charge advertisers accordingly.

> This "content-targeted advertising" based on Google's patented methods was named AdSense. By 2004, AdSense had achieved a run rate of a million dollars a day, and by 2010, it produced annual revenues of more than $10 billion.

Click-through rates soared, and advertising became as important to Google's operations as the search function itself.

It should be noted, however, that the Google's techniques of data acquisition have no more necessary connection with advertising than the principles of mass production had with the Model-T. In the future, plenty of other actors may become interested in behavioral surplus—notably in government.

In 2001, as Google's surveillance advertising strategy was being tested, net revenues more than quadrupled over the previous year, reaching $86 million, and the company turned its first profit. "Revenues leapt to $347 million in 2002, then $1.5 billion in 2003, and $3.5 billion in 2004, the year the company went public."

> The firm's substantial revenue flows summoned the greatest minds of our age from fields such as artificial intelligence, statistics, machine learning, data science, and predictive analytics to converge on the prediction of human behavior.

Google end-users did not need to know anything about Google's surveillance and data gathering techniques: from the company's point of view, it was best if they did not. Employees were bound to secrecy by non-disclosure agreements. Cofounder Larry Page sought

> to avoid arousing users' curiosity by minimizing their exposure to any clues about the reach of the firm's data operations. He questioned the prudence of the electronic scroll in the reception lobby that displays a continuous stream of search queries, and he "tried to kill" the annual Google Zeitgeist conference that summarizes the year's trends in search terms.

Secrecy was easy to maintain in the early days, since few suspected that what Google was doing was even feasible.

Of course, plenty of companies conceal proprietary information from competitors, but Google's secrecy was also motivated by fears of a public backlash against

> its capabilities in unilateral surveillance of online behavior and its methods specifically designed to override individual decision rights. Google policies had to enforce secrecy to protect operations that took things from

> users without asking and employed those unilaterally claimed resources in the service of other's purposes.

U.S. Supreme Court Justice William O. Douglas once wrote that "privacy involves the choice of the individual to disclose or reveal what he believes, what he thinks, what he possesses." From this point of view, Google was not so much eroding users' privacy as appropriating it for themselves. From the very nature of its business, the company was compelled to assert a right to take personal information. Such an assertion might have become matter for public deliberation and negotiation, but Google's secrecy—as well as the frenetic pace of its operations—allowed it to present the public with a *fait accompli* by the time the full nature of its operations was understood.

The company has continually stressed that it does not *sell* users' personal data. This is correct: private data is merely its raw material. What it sells are "predictions that only it can fabricate from its world-historic private hoard of behavioral surplus." Google has also defended its practices with a rhetoric centered on the inevitability of technological progress and neoliberal economics. But this should not fool us: surveillance capitalism is

> neither a necessary development of information capitalism nor a necessary product of digital technology or the internet. It is a specifically constructed human choice, an unprecedented market form, and the underlying mechanism through which a new asset class is created on the cheap and converted to revenue.

The attacks of September 11, 2001, also helped create an atmosphere favorable to data gathering and unfavorable to privacy concerns. Just the year before, the Federal Trade Commission had been expressing concern that only eight percent of popular websites had received a seal of approval from an industry privacy watchdog, and recommending new federal regulations, including: "clear and conspicuous" notice of information practices; consumer choice over how personal information is used; access to all personal information, including the right to correct or delete; and enhanced security of personal information. Following 9/11, such talk stopped "more or less overnight."

> The US Congress passed the Patriot Act and instituted a host of other measures that dramatically increased the warrantless collection of personal information. By late 2001 the intelligence community established "information dominance" in the public's house, quickly institutionalizing it in hundreds of billions of dollars' worth of state-sponsored global technology infrastructure, personnel and practice.

As early as 1999, the CIA had established its own Silicon Valley startup, In-Q-Tel, "as a conduit for cutting-edge technologies." After 9/11, In-Q-Tel went into "a state of hyperactivity," serving the agency as a critical source of new capabilities and relationships with Silicon Valley firms, including Google. In 2003 Google provided the CIA with a customized version of its search engine as part of creating a "top secret intranet." In 2004, Google acquired Keyhole, a satellite mapping company whose initial capitalization had come from In-Q-Tel. Keyhole became the backbone of Google Earth. In 2009 Google and In-Q-Tel both invested in a Boston-based startup, Recorded Future, that monitors every aspect of the web in real time in order to predict future events.

> During these years, scholars noted the growing interdependencies between the intelligence agencies, resentful of constitutional constraints on their prerogatives, and the Silicon Valley firms. The government's need to evade constitutional oversight [led] to secret public-private intelligence collaborations "orchestrated around handshakes rather than legal formalities, such as search warrants, and may be arranged this way to evade oversight and, at times, to defy the law."

During these same years, Google also began taking an interest in electoral politics, with special attention to the presidential ambitions of Barack Obama. Google CEO Eric Schmidt helped his 2008 campaign compile data on 250 million Americans, including "a vast array of online behavioral and relational data collected from use of the campaign's web site and third-party social media sites such as Facebook." One consultant claimed: "We knew who…people were going to vote for before they did."

Schmidt's role in Obama's 2012 reelection was even more prominent:

> The campaign knew "every single wavering voter in the country that it needed to persuade to vote for Obama by name, address, race, sex, and income" and had figured out how to target television ads to these individuals. One breakthrough was the "persuasion score" that identified how easily each undecided voter could be persuaded to vote for the Democratic candidate.

As of April 2016, 197 persons had migrated from the government into the Googlesphere, and 61 had moved in the other direction. These numbers include White House officials and Google executives. The company also spends more on lobbying than any other corporation: $18 million in 2018.

By 2014, Google's $400 billion market value had surpassed ExxonMobil to make it the second richest company in the world. It has since occasionally edged out Apple for the number one spot. The company processes an average of 40,000 search queries every second, equivalent to 1.2 trillion worldwide in 2017. Eighty-nine percent of its revenue comes from its targeted advertising program.

Next to arrive at the feast was Facebook, launched the same year Google went public. Initially aimed at college students, Facebook opened its platform to the entire world in May 2007. Six months later, founder and CEO Mark Zuckerberg announced the creation of Beacon, Facebook's advertising product which automatically (i.e., without the user opting in) shared transactions from partner websites with all a user's "friends," whether the user was logged into Facebook or not, and without the user's knowledge.

> Howls of protest forced Zuckerberg to back down quickly. By December, Beacon became an opt-in program. The twenty-three-year-old CEO understood the potential of surveillance capitalism, but had not yet mastered Google's facility in obscuring its operations and intent.

Just three months later, in March, 2008, Zuckerberg hired Google executive Sheryl Sandberg as Facebook's chief Operating Officer. Sandberg had gone to work at Google in 2001, rising to become its vice president of global online sales and operations: "AdWords" had been her project. She understood that Facebook "represented an awe-inspiring source of behavioral surplus" whose atmosphere of intimacy and sharing could be manipulated to *create* demand where none had previously existed.

Google and Facebook began buying up anything in sight which would allow them to collect more data. In 2006, Google paid $1.65 billion to buy out YouTube, a struggling startup which had never turned a profit and was bogged down in copyright infringement lawsuits. Observers thought the deal was crazy, failing to understand that Google was aiming at YouTube's behavioral surplus.

> Facebook's Zuckerberg pursued the same strategy, paying "astronomical" prices for a parade of typically unprofitable startups like Oculus ($2 billion) and WhatsApp ($19 billion), ensuring Facebook's ownership of the gargantuan flows of human behavior that would pour through these pipes.

The companies have since invested in such seemingly mission-irrelevant things as smart-home devices, wearables, self-driving cars, and drones.

Google has gradually developed its own content, including its own price results for shopping and reviews for local businesses, and its search function systematically favors this content over that of competitors. They have also developed a product called Google Toolbar, whose "enhanced features" transmit to the company "the full URL of every page view, including searches at competing search engines." Researchers found it was "strikingly easy" to activate the toolbar's "enhanced features," but impossible to disable them afterwards: "Even when a user specifically instructed that the toolbar be disabled, and even when it appeared to be disabled because it had disappeared from view, the toolbar continued to track browsing behavior."

Disconnect, Inc. is an Internet privacy company founded in 2011 by two former Google engineers and a privacy-rights attorney. They develop apps to protect the privacy and security of Internet users by blocking "invisible, unsolicited and frequently undisclosed" network connections from third party sites and services of the sort that now occur whenever a user visits a website or opens a mobile application.

In 2015, the Disconnect team found that anyone who simply visited the 100 most popular websites would collect over 6,000 cookies in his computer, 83 percent of which were from third parties unrelated to the website visited. The team found Google tracking infrastructure on 92 of the top hundred, and 923 of the top thousand websites. Google has banned Disconnect software from Google Play's vast catalogue of mobile apps, leading to a lawsuit that is still ongoing.

In 2007 Google announced an important new addition to its Google Maps service: "Street View." The company employs cars with large 360-degree camera mounts on the roof to capture images of houses and storefronts on ordinary streets all over the world. By January 2009, Germany and Japan were protesting. That April, citizens of tiny Broughton, England physically blocked a Street View car at the village perimeter.

> In 2010 the German Federal Commission for Data Protection announced that Street View cars were secretly collecting personal data from private Wi-Fi networks. Google denied the charge. Within days, an independent analysis proved decisively that Street View's cars were extracting unencrypted personal information from homes. [Such data could include] names, telephone numbers, credit information, passwords, messages, e-mails, and chat transcripts, as well as records of online dating, pornography, browsing behavior, medical information, location, photos, and video and audio files.

The company was forced to admit that it had made

a "mistake," blaming it on a single engineer working on an "experimental" project, whose code had inadvertently made it into Street View's software.

> The FCC found evidence that contradicted Google's scapegoating narrative. The records showed that the engineer had e-mailed links to his software documentation to project leaders, who then shared them with the entire Street View team. It also found evidence that on at least two occasions, the engineer had told his colleagues that Street View was collecting personal data.

Street View has since been banned in Germany, Austria, the Czech Republic, Greece, Lithuania, and India. The author reports, however, that by the summer of 2017, Street View data had mysteriously reappeared for "at least some regions of each of these countries."

Space does not permit us to recount how, since about 2014, Microsoft, Verizon, Comcast, and others have joined the stampede toward collecting personal data. Surveillance software can now be programmed to bypass or override all signals of a user's intentions. There are now cookies which recreate themselves whenever they are deleted, and "indoor positioning systems" that track individual movements in airports, shopping malls, and retail stores. For ordinary people, concludes one researcher, "there is simply no defense." ■

Zuckerberg Calls for More Regulations and 'Thought Control'

While Investors Are Warned: He 'May Be the Greatest Con Man in History'

WAYNE LUTTON

At the end of March, Facebook, Inc. CEO Mark Zuckerberg called for global regulators to take a "more active role" in governing the Internet, saying that governments need to set clearer rules on "harmful content, election integrity, privacy and data portability." Zuckerberg said such intervention is "vital to protect both the welfare of users and the fundamental values of an open Internet," as reported in the *Wall Street Journal* (April 1, p. B1). In other words, big government should be given even more power over the information and opinion available to individuals through tech giants that cooperate with those very governments.

As readers may be aware, public officials in a number of countries are calling for the breakup of Facebook and similar mass technology companies. The editors of the *Wall Street Journal* ["Zuckerberg for Regulation," April 1, 2019, p. A 16] recently suggested that his "plea for big government to regulate big business will go down well in liberal precincts, where the tech giants have lost the political immunity they had during the Obama years…. Mr. Zuckerberg may think he is buying some protection" from calls to apply antitrust standards to his operations.

Zuckerberg further pledged to do more to "suppress hate speech and other forms of harmful content on its platform." On March 27, 2019 Facebook executives disclosed that they had spent over three months discussing how to police the Internet with un-named (leftist) academics and "civil-rights" groups (such as the discredited Southern Poverty Law Center). Facebook pledged to begin banning even more content that these highly partisan censors charge contributes to "hate speech and misinformation." In early April, Facebook started redirecting people who search for terms their censors associate with "white supremacy" and "white nationalism" to an outfit called "Life After Hate."

On April 3, 2019, Bloomberg.com financial news reported that the personal records, including financial data, of millions of Facebook users were "hiding in plain sight" and posted publicly on Amazon.com Inc.'s cloud computing servers. One Mexico City-based digital platform, Cultura Colectiva, openly stored the records of 540 million Facebook users, including identification numbers and account names. The records were accessible and downloadable for anyone who could find them online. There was little to stop foreign intelligence services, political spying operations, telemarketers, grifters, salesmen, sexual predators, and psychopaths from accessing this information.

Aaron Greenspan, in a PlainSite Reality Check report on Facebook, Inc., reviewed the history of Facebook since Mark Zuckberg claims he created it in his Harvard dorm room in 2004. Greenspan warned readers that "Facebook's deception goes back so far and is so pervasive that cataloging its full scope is nearly impossible…. The truth is that at this point, Mark Zuckerberg may in fact be the greatest con man in history, having pulled off a complex fraud at one point valued at approximately ten times the scale of convicted financier Bernard Madoff's historic and epic Ponzi scheme." ■

[See www.plainsite.org/realitycheck/Facebook,Inc. PlainSite is a legal research initiative.]