

traduzione automatica. sotto lingua originale, foto e links

foreignaffairs.com/  
Novembre / dicembre 2019

## **I nuovi padroni dell'universo Big Tech e il business della sorveglianza di Paul Starr**

Nel suo classico del 1944, *The Great Transformation*, lo storico economico Karl Polanyi raccontò la storia del capitalismo moderno come un "doppio movimento" che portò sia all'espansione del mercato che alla sua restrizione. Durante il diciottesimo e l'inizio del diciannovesimo secolo, le vecchie restrizioni feudali al commercio furono abolite e la terra, il lavoro e il denaro vennero trattati come merci. Ma il capitalismo sfrenato ha devastato l'ambiente, danneggiato la salute pubblica e portato a panici economici e depressioni, e quando Polanyi scriveva, le società avevano reintrodotta i limiti sul mercato.

Shoshana Zuboff, professoressa emerita alla Harvard Business School, vede una nuova versione della prima metà del doppio movimento di Polanyi all'opera oggi con l'ascesa del "capitalismo della sorveglianza", una nuova forma di mercato sperimentata da Facebook e Google. In *The Age of Surveillance Capitalism*, sostiene che il capitalismo sta ancora una volta estendendo la sfera del mercato, questa volta rivendicando "l'esperienza umana come materia prima gratuita per pratiche commerciali nascoste di estrazione, previsione e vendita". Con l'ascesa dell'"ubiquitous computing" (la diffusione dei computer in tutti i regni della vita) e dell'Internet of Things (la connessione di oggetti quotidiani a Internet), l'estrazione dei dati è diventata pervasiva. Viviamo in un mondo sempre più popolato di dispositivi in rete che catturano le nostre comunicazioni, movimenti, comportamenti e relazioni, persino le nostre emozioni e stati d'animo. E, avverte Zuboff, il capitalismo della sorveglianza è finora sfuggito al tipo di contromovimento descritto da Polanyi.

I dispositivi in rete catturano le nostre comunicazioni, movimenti, comportamenti e relazioni.

Il libro di Zuboff è un'analisi brillante e sorprendente dell'economia digitale e un appello per un risveglio sociale sull'enormità dei cambiamenti che la tecnologia sta imponendo alla vita politica e sociale. La maggior parte degli americani vede le minacce rappresentate dalle società tecnologiche come questioni di privacy. Ma Zuboff mostra che il capitalismo della sorveglianza implica più che l'accumulo di dati personali su una scala senza precedenti. Le aziende tecnologiche e i loro esperti - che Zuboff chiama "il nuovo sacerdozio" - stanno creando nuove forme di potere e mezzi di modifica comportamentale che operano al di fuori della consapevolezza individuale e della responsabilità pubblica. Il controllo del potere di questo sacerdozio richiederà un nuovo movimento contrario, che limiti il capitalismo di sorveglianza in nome della libertà personale e della democrazia.

### **L'ASCESA DELLE MACCHINE**

È già in corso una reazione contro il potere dell'industria tecnologica. Il Dipartimento di Giustizia degli Stati Uniti e la Federal Trade Commission stanno conducendo indagini antitrust su Amazon, Apple, Facebook e Google. A luglio, la FTC ha imposto una multa di 5 miliardi di dollari a Facebook per aver violato le promesse ai consumatori che l'azienda aveva fatto nelle proprie politiche sulla privacy (gli Stati Uniti, a differenza dell'Unione Europea, non hanno leggi generali che proteggano la privacy online). Il Congresso sta prendendo in considerazione una legislazione per limitare l'uso dei dati da parte delle società tecnologiche e annullare l'ampia immunità dalla responsabilità per i contenuti generati dagli utenti che ha concesso loro nel Communications Decency Act del 1996. Questo dibattito nazionale, ancora incerto nel suo impatto finale, fa sì che Zuboff prenda in modo ancora più tempestivo e pertinente.

L'ascesa del capitalismo della sorveglianza ha anche una dimensione internazionale. Le aziende statunitensi hanno dominato a lungo l'industria tecnologica e Internet, suscitando sospetti e opposizione in altri paesi. Ora, castigati dall'esperienza dell'interferenza russa nelle elezioni presidenziali statunitensi del 2016, gli americani si innervosiscono per l'archiviazione di dati personali che cadono nelle mani di potenze straniere ostili. Nel luglio di quest'anno, c'è stato un panico virale su FaceApp, un'applicazione mobile per la modifica di immagini di volti che milioni di americani avevano scaricato per vedere le immagini proiettate di se stessi in età avanzata. Creata da un'azienda russa, si diceva che l'app fosse utilizzata dall'intelligence russa per raccogliere dati sul riconoscimento facciale, forse per creare video deepfake, voci che l'azienda ha negato. All'inizio dello scorso anno, l'acquisizione da parte di una società cinese dell'app di incontri gay Grindr ha suscitato preoccupazione per il potenziale utilizzo dei dati dell'app per compromettere le persone e la sicurezza nazionale degli Stati Uniti; il Comitato federale per gli investimenti esteri negli Stati Uniti ha da allora ordinato all'azienda cinese di evitare l'accesso ai dati di Grindr e di disinvestirsi interamente di Grindr entro giugno 2020. Non è difficile immaginare come la rivalità tra Stati Uniti e Cina potrebbe portare non solo a un divorzio tecnologico ma anche a due mondi diversi della sorveglianza quotidiana.

Secondo Zuboff, il capitalismo della sorveglianza è nato dalle brillanti scoperte e dalle sfacciate affermazioni di un'azienda americana. "Google", scrive, "è per il capitalismo di sorveglianza quello che la Ford Motor Company e la General Motors erano per il capitalismo manageriale basato sulla produzione di massa". Incorporata nel 1998, Google divenne presto il dominio della ricerca su Internet. Ma inizialmente non si concentrava sulla pubblicità e non aveva un percorso chiaro per la redditività. Quello che aveva era un'analisi rivoluzionaria: i dati collaterali derivati dalle ricerche (il numero e i modelli di query, le loro frasi, i modelli di clic delle persone e così via) potevano essere utilizzati per migliorare i risultati di ricerca di Google e aggiungere nuovi servizi per gli utenti. Ciò attirerebbe più utenti, il che a sua volta migliorerebbe ulteriormente il suo motore di ricerca in un ciclo ricorsivo di apprendimento ed espansione.

La svolta commerciale di Google è avvenuta nel 2002, quando ha visto che poteva anche utilizzare i dati collaterali raccolti per profilare gli utenti stessi in base alle loro caratteristiche e interessi. Quindi, invece di abbinare gli annunci alle query di ricerca, l'azienda potrebbe abbinare gli annunci ai singoli utenti. Il targeting degli annunci in modo preciso ed efficiente per le persone è il Santo Graal della pubblicità. Piuttosto che essere clienti di Google, sostiene Zuboff, gli utenti sono diventati i suoi fornitori di materie prime, da cui l'azienda ha ricavato quello che lei chiama "surplus comportamentale". Tale surplus è costituito dai dati al di sopra e al di là di ciò di cui Google ha bisogno per migliorare i servizi per gli utenti. Insieme alle formidabili capacità dell'azienda nell'intelligenza artificiale, gli enormi flussi di dati di Google hanno permesso di creare quella che Zuboff vede come la vera base del settore della sorveglianza: "prodotti di previsione", che anticipano ciò che gli utenti faranno "ora, presto e dopo." Prevedere ciò che le persone acquisteranno è la chiave per la pubblicità, ma le previsioni comportamentali hanno un valore evidente anche per altri scopi, come assicurazioni, decisioni di assunzione e campagne politiche.

L'analisi di Zuboff aiuta a dare un senso ai servizi apparentemente non correlati offerti da Google, alle sue diverse iniziative e alle numerose acquisizioni. Gmail, Google Maps, il sistema operativo Android, YouTube, Google Home, persino auto a guida autonoma: questi e dozzine di altri servizi sono tutti modi, sostiene Zuboff, di espandere le "rotte di approvvigionamento" dell'azienda per gli utenti dati sia online che offline. Chiedere il permesso per ottenere tali dati non faceva parte dello stile operativo dell'azienda. Ad esempio, quando l'azienda stava sviluppando Street View, una funzionalità del suo servizio di mappatura che mostra fotografie di luoghi diversi, è andata avanti e ha registrato immagini di strade e case in diversi paesi senza prima chiedere il permesso locale,

combattendo l'opposizione non appena si presentava. . Nel settore della sorveglianza, qualsiasi area indifesa della vita sociale è un gioco leale.

Questo modello di espansione riflette una logica sottostante del settore: nella competizione per i ricavi dell'intelligenza artificiale e della sorveglianza, il vantaggio va alle aziende che possono acquisire flussi di dati sia vasti che diversificati. Anche le altre società impegnate nel capitalismo della sorveglianza ai massimi livelli - Amazon, Facebook, Microsoft e le grandi società di telecomunicazioni - devono affrontare gli stessi imperativi espansivi. Passo dopo passo, l'industria ha ampliato sia l'ambito della sorveglianza (migrando dal mondo virtuale a quello reale) sia la profondità della sorveglianza (scandagliando gli interni delle vite degli individui e accumulando dati sulle loro personalità, umori ed emozioni) .

Il settore della sorveglianza non ha dovuto affrontare molte resistenze perché agli utenti piacciono le sue informazioni personalizzate e i prodotti gratuiti. In effetti, gli piacciono così tanto che accettano prontamente termini di servizio onerosi e unilaterali. Quando è esplosa la controversia su Facebook, molte persone che avevano utilizzato l'app sono rimaste sorprese di apprendere di aver accettato di dare alla società "una licenza perpetua, irrevocabile, non esclusiva, priva di royalty, mondiale, interamente pagata, trasferibile in sublicenza a utilizzare, riprodurre, modificare, adattare, pubblicare, tradurre, creare opere derivate da, distribuire, eseguire pubblicamente e visualizzare i tuoi Contenuti utente e qualsiasi nome, nome utente o somiglianza fornito in relazione al tuo Utente, Contenuti in tutti i formati e canali multimediali ora conosciuti o sviluppati in seguito, senza alcun compenso per te ". Ma questa non era una subdola formulazione russa. Come ha sottolineato Wired , Facebook ha termini di servizio altrettanto onerosi.

Anche se il Congresso promulgasse leggi che vietano alle aziende di imporre termini così estremi, è improbabile che risolva i problemi sollevati da Zuboff. La maggior parte delle persone è probabilmente disposta ad accettare l'uso dei dati per personalizzare i propri servizi e visualizzare la pubblicità che si prevede possa essere di loro interesse, ed è improbabile che il Congresso lo fermi. Gli stessi processi di personalizzazione, tuttavia, possono essere utilizzati per modificare comportamenti e convinzioni. Questa è la preoccupazione principale del libro di Zuboff: la creazione di un sistema di potere e dominio in gran parte nascosto.

## **FARLI BALLARE**

Dall'estrazione dei dati e dalla formulazione di previsioni, le aziende tecnologiche sono passate a intervenire nel mondo reale. Dopo tutto, quale modo migliore per migliorare le previsioni che guidare il modo in cui le persone agiscono? Il termine del settore per plasmare il comportamento è "attuazione". Alla ricerca dell'attivazione, scrive Zuboff, le aziende tecnologiche "spingono, sintonizzano, raggruppano, manipolano e modificano il comportamento in direzioni specifiche eseguendo azioni sottili come l'inserimento di una frase specifica nel feed di notizie di Facebook, temporizzando la comparsa di un pulsante ACQUISTA su il telefono o spegnendo il motore dell'auto quando il pagamento dell'assicurazione è in ritardo. "

La prova della capacità dell'industria di modificare il comportamento su larga scala proviene da due studi condotti da Facebook. Durante le elezioni del Congresso degli Stati Uniti del 2010, i ricercatori dell'azienda hanno condotto un esperimento controllato e randomizzato su 61 milioni di utenti. Gli utenti sono stati suddivisi in tre gruppi. A due gruppi sono state mostrate informazioni sul voto (come l'ubicazione dei seggi elettorali) nella parte superiore dei loro feed di notizie di Facebook; Gli utenti di uno di questi gruppi hanno ricevuto anche un messaggio social contenente fino a sei foto di amici di Facebook che avevano già votato. Il terzo gruppo non ha ricevuto informazioni speciali sulla votazione. L'intervento ha avuto un effetto significativo su coloro che hanno ricevuto il messaggio sociale: i ricercatori hanno stimato che l'esperimento ha portato a 340.000 voti

aggiuntivi. In un secondo esperimento, i ricercatori di Facebook hanno adattato il contenuto emotivo dei feed di notizie degli utenti, in alcuni casi riducendo il numero di post di amici che esprimono emozioni positive e in altri casi riducendo i loro post negativi. Hanno scoperto che coloro che hanno visualizzato più post negativi nei loro feed di notizie hanno continuato a pubblicare loro stessi post più negativi, dimostrando, come dice il titolo dell'articolo pubblicato sullo studio, "contagio emotivo su vasta scala attraverso i social network".

La Brexit del 2016 e le elezioni statunitensi hanno fornito esempi reali di disinformazione occulta trasmessa tramite Facebook. Non solo la società aveva precedentemente consentito alla società di consulenza politica Cambridge Analytica di raccogliere dati personali su decine di milioni di utenti di Facebook; durante le elezioni statunitensi del 2016, ha anche consentito il microtargeting di "annunci di post di pagina non pubblicati", generalmente noti come "post oscuri", che erano invisibili al grande pubblico. Questi sono stati forniti agli utenti come parte dei loro feed di notizie insieme al contenuto normale e quando gli utenti li hanno apprezzati, commentati o condivisi, i loro amici hanno visto gli stessi annunci, ora approvati personalmente. Ma i post oscuri sono poi scomparsi e non sono mai stati archiviati pubblicamente. Il micro-targeting degli annunci non è intrinsecamente illegittimo, ma i giornalisti non sono in grado di controllare l'inganno e gli oppositori politici non possono respingere gli attacchi quando i social media trasmettono tali messaggi al di fuori della sfera pubblica. La diffusione di disinformazione segreta su base di massa è fondamentalmente ostile al dibattito democratico.

Da allora Facebook ha eliminato i post oscuri e ha apportato altre modifiche in risposta alle critiche pubbliche, ma Zuboff ha ancora ragione su questo punto centrale: "Facebook possiede un mezzo senza precedenti di modifica del comportamento che opera di nascosto, su larga scala e in assenza di meccanismi di accordo, contestazione e controllo." Nessuna legge, ad esempio, vieta a Facebook di modificare i feed di notizie dei suoi utenti per favorire un partito politico o un altro (e negli Stati Uniti, una legge del genere potrebbe essere considerata incostituzionale). Come ha dimostrato uno studio del 2018 del Wall Street Journal, l'algoritmo di raccomandazione di YouTube forniva agli spettatori video di gruppi marginali sempre più estremi. Quell'algoritmo e altri rappresentano un'enorme fonte di potere su credenze e comportamenti.

Il capitalismo della sorveglianza, secondo Zuboff, sta muovendo la società in una direzione fondamentalmente antidemocratica. Con l'avvento dell'ubiquità informatica, l'industria sogna di creare sistemi di trasporto e intere città con meccanismi integrati per il controllo del comportamento. Utilizzando sensori, fotocamere e dati sulla posizione, Sidewalk Labs, una consociata della società madre di Google, Alphabet, immagina una "città a scopo di lucro" con i mezzi per far rispettare le normative cittadine e con mercati online dinamici per i servizi cittadini. Il sistema richiederebbe alle persone di utilizzare il sistema di pagamento mobile di Sidewalk e consentirebbe all'azienda, come ha spiegato il suo CEO, Dan Doctoroff, in un discorso del 2016, di "indirizzare gli annunci alle persone nelle vicinanze e quindi ovviamente nel tempo seguirli attraverso cose come beacon e servizi di localizzazione e la loro attività di navigazione." Uno sviluppatore di software per una società di Internet of Things ha detto a Zuboff: "Stiamo imparando a scrivere la musica e poi lasciamo che la musica le faccia ballare".

Tali aspirazioni implicano una radicale disuguaglianza di potere tra le persone che controllano la playlist e le persone che la ballano. Nell'ultimo terzo del suo libro, Zuboff porta la sua analisi a un livello superiore, identificando le idee teoriche e il modello generale di società che vede come impliciti nel capitalismo della sorveglianza. L'idea che anima il capitalismo della sorveglianza, dice Zuboff, è quella dello psicologo BF Skinner, che considerava la fede nella libertà umana come un'illusione che ostacolava un mondo più armonioso e controllato. Ora, secondo Zuboff, l'industria tecnologica sta sviluppando i mezzi di modifica del comportamento per realizzare il programma di Skinner.

Il sistema emergente di dominio, avverte Zuboff, non è totalitario; non ha bisogno di violenza e non ha interesse per la conformità ideologica. Invece, è ciò che lei chiama "strumentista": usa la sorveglianza e l'attivazione quotidiana per incanalare le persone nelle direzioni preferite da chi ha il controllo. Ad esempio, descrive gli sforzi della Cina per introdurre un sistema di credito sociale che valuti gli individui in base al loro comportamento, ai loro amici e ad altri aspetti della loro vita e quindi utilizza questo punteggio per determinare l'accesso di ogni individuo a servizi e privilegi. Il sistema cinese fonde il potere strumentale e lo stato (ed è interessato alla conformità politica), ma la sua emergente controparte americana può fondere il potere strumentale e il mercato.

### **SENZA FUTURO?**

*The Age of Surveillance Capitalism* è un libro potente e appassionato, il prodotto di una profonda immersione sia nella tecnologia che negli affari che è anche informato da una comprensione della storia e da un impegno per la libertà umana. Zuboff sembra, tuttavia, incapace di resistere alle più terribili ed esagerate formulazioni della sua argomentazione. Scrive, ad esempio, che il settore è passato "dall'automazione dei flussi di informazioni su di te all'automazione di te". Un sistema strumentale di modifica del comportamento, dice, non è solo una possibilità, ma un'inevitabilità, guidata dalla logica interna del capitalismo di sorveglianza: "Proprio come il capitalismo industriale è stato spinto alla continua intensificazione dei mezzi di produzione, così i capitalisti di sorveglianza lo sono. . . ora bloccato in un ciclo di intensificazione continua dei mezzi di modifica comportamentale. "

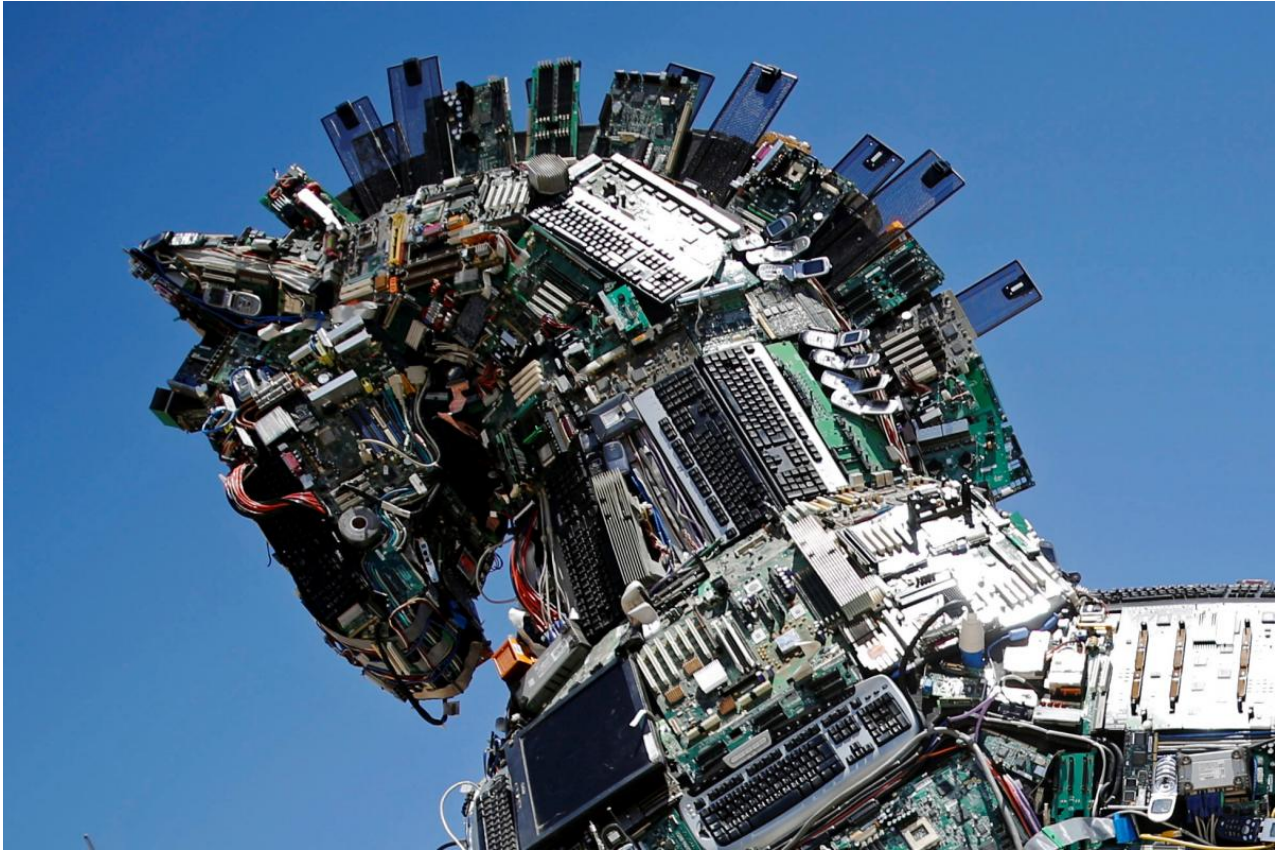
Come avvertimento, l'argomento di Zuboff merita di essere ascoltato, ma gli americani sono tutt'altro che semplici burattini nelle mani della Silicon Valley. Il puzzle qui è che Zuboff rifiuta una retorica di "inevitabilità" - "la dittatura di nessuna alternativa" - ma il suo libro dà poche basi per pensare che possiamo evitare le nuove tecnologie di controllo, e lei stessa ha poco da dire su alternative specifiche. Profezia che troverai qui; politica, non così tanto. Sostiene giustamente che smantellare le grandi società tecnologiche non risolverebbe i problemi che solleva, sebbene l'azione antitrust possa essere giustificata per altri motivi. Alcuni riformatori hanno suggerito di creare una struttura normativa completamente nuova per gestire la potenza delle piattaforme digitali e migliorare la "responsabilità algoritmica", ovvero identificare e porre rimedio ai danni degli algoritmi. Ma tutto questo è al di fuori di questo libro.

Gli americani sono tutt'altro che semplici burattini nelle mani della Silicon Valley. Più potere eserciteranno le principali piattaforme tecnologiche sulla politica e sulla società, maggiore sarà l'opposizione che provocherà, non solo negli Stati Uniti ma anche in tutto il mondo. La portata globale del capitalismo di sorveglianza americano potrebbe essere solo una fase temporanea. Il nazionalismo è in marcia oggi e l'industria tecnologica è sul suo cammino: i paesi che vogliono tracciare il proprio destino non continueranno a consentire alle aziende statunitensi di controllare le loro piattaforme di comunicazione e politica. La concorrenza di aziende e sistemi politici rivali può anche complicare qualsiasi tentativo di riformare l'industria tecnologica negli Stati Uniti. Sarebbe una buona cosa, ad esempio, regolamentare pesantemente le principali aziende tecnologiche statunitensi se i loro rivali cinesi guadagnassero di conseguenza? Le società statunitensi professano almeno valori democratici liberali. Il trucco è approvare leggi per mantenerli a questi valori. Se il libro di Zuboff aiuta a risvegliare un contromovimento per ottenere quel risultato, potremmo ancora essere in grado di evitare il futuro oscuro che vede nascere oggi.

# Big Tech and the Business of Surveillance

 [foreignaffairs.com/reviews/review-essay/2019-10-10/new-masters-universe](https://foreignaffairs.com/reviews/review-essay/2019-10-10/new-masters-universe)

July 29, 2020



---

## **The New Masters of the Universe Big Tech and the Business of Surveillance By Paul Starr**

**November/December 2019**

In his 1944 classic, *The Great Transformation*, the economic historian Karl Polanyi told the story of modern capitalism as a “double movement” that led to both the expansion of the market and its restriction. During the eighteenth and early nineteenth centuries, old feudal restraints on commerce were abolished, and land, labor, and money came to be treated as commodities. But unrestrained capitalism ravaged the environment, damaged public health, and led to economic panics and depressions, and by the time Polanyi was writing, societies had reintroduced limits on the market.

Shoshana Zuboff, a professor emerita at the Harvard Business School, sees a new version of the first half of Polanyi’s double movement at work today with the rise of “surveillance capitalism,” a new market form pioneered by Facebook and Google. In *The Age of Surveillance Capitalism*, she argues that capitalism is once again extending the sphere of the market, this time by claiming “human experience as free raw material for hidden commercial practices of extraction, prediction, and sales.” With the rise of “ubiquitous computing” (the spread of computers into all realms of life) and the Internet of Things (the connection of everyday objects to the Internet), the extraction of data has become pervasive. We live in a world increasingly populated with networked devices that capture our communications, movements, behavior, and relationships, even our emotions and states of mind. And, Zuboff warns, surveillance capitalism has thus far escaped the sort of countermovement described by Polanyi.

| Networked devices capture our communications, movements, behavior, and relationships.

Zuboff’s book is a brilliant, arresting analysis of the digital economy and a plea for a social awakening about the enormity of the changes that technology is imposing on political and social life. Most Americans see the threats posed by technology companies as matters of privacy. But Zuboff shows that surveillance capitalism involves more than the accumulation of personal data on an unprecedented scale. The technology firms and their experts—whom Zuboff labels “the new priesthood”—are creating new forms of power and means of behavioral modification that operate outside individual awareness and public accountability. Checking this priesthood’s power will require a new countermovement—one that restrains surveillance capitalism in the name of personal freedom and democracy.

## THE RISE OF THE MACHINES

---

A reaction against the power of the technology industry is already underway. The U.S. Justice Department and the Federal Trade Commission are conducting antitrust investigations of Amazon, Apple, Facebook, and Google. In July, the FTC levied a \$5 billion fine on Facebook for violating promises to consumers that the company made in its own privacy policies (the United States, unlike the European Union, has no general law protecting online privacy). Congress is considering legislation to limit technology companies’ use of data and roll back the broad immunity from liability for user-generated content that it granted them in the Communications Decency Act of 1996. This national debate, still uncertain in its ultimate impact, makes Zuboff’s book all the more timely and relevant.

The rise of surveillance capitalism also has an international dimension. U.S. companies have long dominated the technology industry and the Internet, arousing suspicion and opposition in other countries. Now, chastened by the experience of Russian interference in the 2016 U.S. presidential election, Americans are getting nervous about stores of personal data falling into the hands of hostile foreign powers. In July of this year, there was a viral panic about FaceApp, a mobile application for editing pictures of faces that millions of Americans had downloaded to see projected images of themselves at older ages. Created by a Russian firm, the app was rumored to be used by Russian intelligence to gather facial recognition data, perhaps to create deepfake videos—rumors that the firm has denied. Early last year, a Chinese company’s acquisition of the gay dating app Grindr stirred concern about the potential use of the app’s data to compromise individuals and U.S. national security; the federal Committee on Foreign Investment in the United States has since ordered the Chinese firm to avoid accessing Grindr’s data and divest itself entirely of Grindr by June 2020. It is not hard to imagine how the rivalry between the United States and China could lead not only to a technology divorce but also to two different worlds of everyday surveillance.

According to Zuboff, surveillance capitalism originated with the brilliant discoveries and brazen claims of one American firm. “Google,” she writes, “is to surveillance capitalism what the Ford Motor Company and General Motors were to mass-production-based managerial capitalism.” Incorporated in 1998, Google soon came to dominate Internet search. But initially, it did not focus on advertising and had no clear path to profitability. What it did have was a groundbreaking insight: the collateral data it derived from searches—the numbers and patterns of queries, their phrasing, people’s click patterns, and so on—could be used to improve Google’s search results and add new services for users. This would attract more users, which would in turn further improve its search engine in a recursive cycle of learning and expansion.

Google’s commercial breakthrough came in 2002, when it saw that it could also use the collateral data it collected to profile the users themselves according to their characteristics and interests. Then, instead of matching ads with search queries, the company could match ads with individual users. Targeting ads precisely and efficiently to individuals is the Holy Grail of advertising. Rather than being Google’s customers, Zuboff argues, the users became its raw-material suppliers, from whom the firm derived what she calls “behavioral surplus.” That surplus consists of the data above and beyond what Google needs to improve user services. Together with the company’s formidable capabilities in artificial intelligence, Google’s enormous flows of data enabled it to create what Zuboff sees as the true basis of the surveillance industry—“prediction products,” which anticipate what users will do “now, soon, and later.” Predicting what people will buy is the key to advertising, but behavioral predictions have obvious value for other purposes, as well, such as insurance, hiring decisions, and political campaigns.

Zuboff’s analysis helps make sense of the seemingly unrelated services offered by Google, its diverse ventures and many acquisitions. Gmail, Google Maps, the Android operating system, YouTube, Google Home, even self-driving cars—these and dozens of other services are all ways, Zuboff argues, of expanding the company’s “supply routes” for user



data both on- and offline. Asking for permission to obtain those data has not been part of the company's operating style. For instance, when the company was developing Street View, a feature of its mapping service that displays photographs of different locations, it went ahead and recorded images of streets and homes in different countries without first asking for local permission, fighting off opposition as it arose. In the surveillance business, any undefended area of social life is fair game.

This pattern of expansion reflects an underlying logic of the industry: in the competition for artificial intelligence and surveillance revenues, the advantage goes to the firms that can acquire both vast and varied streams of data. The other companies engaged in surveillance capitalism at the highest level—Amazon, Facebook, Microsoft, and the big telecommunications companies—also face the same expansionary imperatives. Step by step, the industry has expanded both the scope of surveillance (by migrating from the virtual into the real world) and the depth of surveillance (by plumbing the interiors of individuals' lives and accumulating data on their personalities, moods, and emotions).

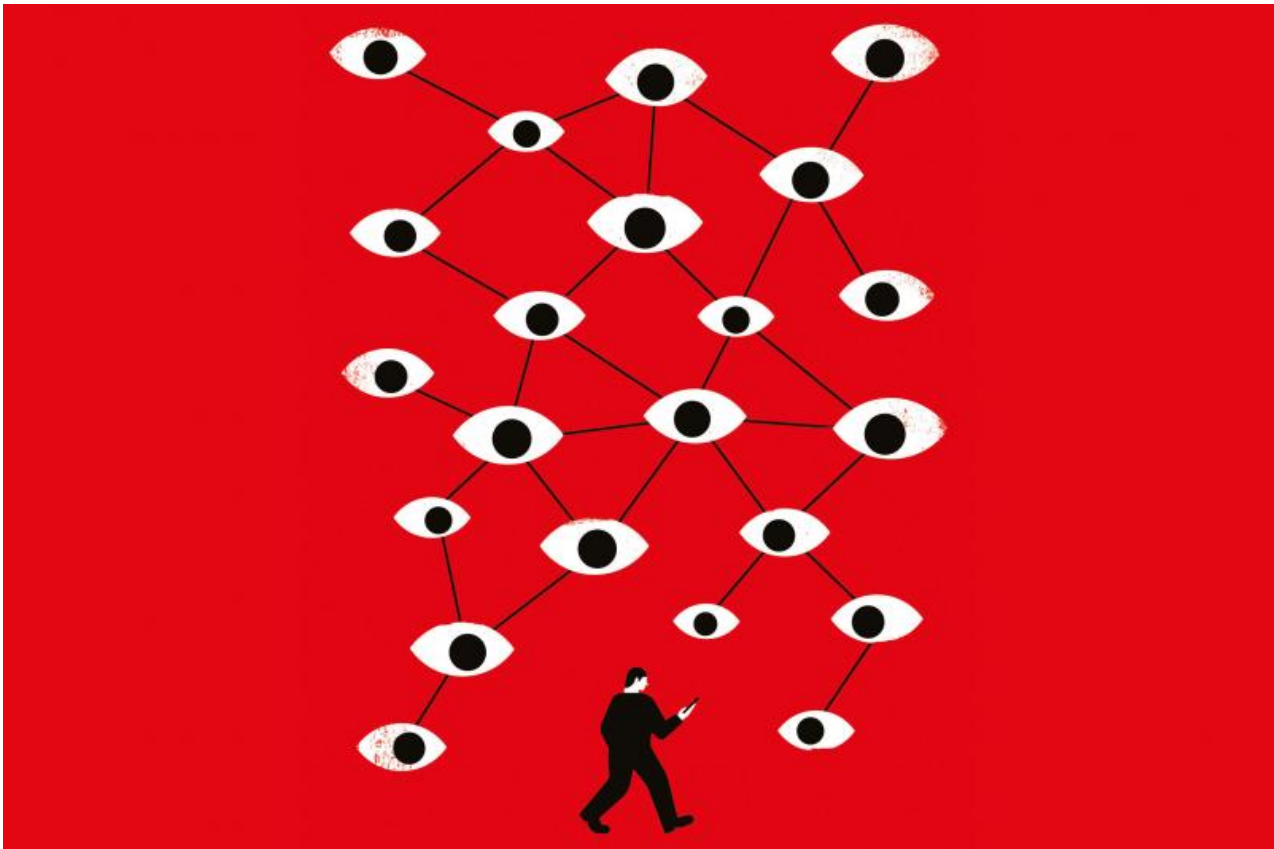


Illustration by the Project Twins

The surveillance industry has not faced much resistance because users like its personalized information and free products. Indeed, they like them so much that they readily agree to onerous, one-sided terms of service. When the FaceApp controversy blew up, many people who had used the app were surprised to learn that they had agreed to give the company “a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User

Content in all media formats and channels now known or later developed, without compensation to you.” But this wasn’t some devious Russian formulation. As *Wired* pointed out, Facebook has just as onerous terms of service.

Even if Congress enacts legislation barring companies from imposing such extreme terms, it is unlikely to resolve the problems Zuboff raises. Most people are probably willing to accept the use of data to personalize their services and display advertising predicted to be of interest to them, and Congress is unlikely to stop that. The same processes of personalization, however, can be used to modify behavior and beliefs. This is the core concern of Zuboff’s book: the creation of a largely covert system of power and domination.

## **MAKE THEM DANCE**

---

From extracting data and making predictions, the technology firms have gone on to intervening in the real world. After all, what better way to improve predictions than to guide how people act? The industry term for shaping behavior is “actuation.” In pursuit of actuation, Zuboff writes, the technology firms “nudge, tune, herd, manipulate, and modify behavior in specific directions by executing actions as subtle as inserting a specific phrase into your Facebook news feed, timing the appearance of a BUY button on your phone, or shutting down your car engine when an insurance payment is late.”

Evidence of the industry’s capacity to modify behavior on a mass scale comes from two studies conducted by Facebook. During the 2010 U.S. congressional elections, the company’s researchers ran a randomized, controlled experiment on 61 million users. Users were split up into three groups. Two groups were shown information about voting (such as the location of polling places) at the top of their Facebook news feeds; users in one of these groups also received a social message containing up to six pictures of Facebook friends who had already voted. The third group received no special voting information. The intervention had a significant effect on those who received the social message: the researchers estimated that the experiment led to 340,000 additional votes being cast. In a second experiment, Facebook researchers tailored the emotional content of users’ news feeds, in some cases reducing the number of friends’ posts expressing positive emotions and in other cases reducing their negative posts. They found that those who viewed more negative posts in their news feeds went on to make more negative posts themselves, demonstrating, as the title of the published article about the study put it, “massive-scale emotional contagion through social networks.”

The 2016 Brexit and U.S. elections provided real-world examples of covert disinformation delivered via Facebook. Not only had the company previously allowed the political consulting firm Cambridge Analytica to harvest personal data on tens of millions of Facebook users; during the 2016 U.S. election, it also permitted microtargeting of “unpublished page post ads,” generally known as “dark posts,” which were invisible to the public at large. These were delivered to users as part of their news feeds along with regular content, and when users liked, commented on, or shared them, their friends saw the same ads, now personally endorsed. But the dark posts then disappeared and were never publicly archived. Micro-targeting of ads is not inherently illegitimate, but

journalists are unable to police deception and political opponents cannot rebut attacks when social media deliver such messages outside the public sphere. The delivery of covert disinformation on a mass basis is fundamentally inimical to democratic debate.

Facebook has since eliminated dark posts and made other changes in response to public criticism, but Zuboff is still right about this central point: “Facebook owns an unprecedented means of behavior modification that operates covertly, at scale, and in the absence of social or legal mechanisms of agreement, contest, and control.” No law, for example, bars Facebook from adjusting its users’ news feeds to favor one political party or another (and in the United States, such a law might well be held unconstitutional). As a 2018 study by *The Wall Street Journal* showed, YouTube’s recommendation algorithm was feeding viewers videos from ever more extreme fringe groups. That algorithm and others represent an enormous source of power over beliefs and behavior.

Surveillance capitalism, according to Zuboff, is moving society in a fundamentally antidemocratic direction. With the advent of ubiquitous computing, the industry dreams of creating transportation systems and whole cities with built-in mechanisms for controlling behavior. Using sensors, cameras, and location data, Sidewalk Labs, a subsidiary of Google’s parent company, Alphabet, envisions a “for-profit city” with the means of enforcing city regulations and with dynamic online markets for city services. The system would require people to use Sidewalk’s mobile payment system and allow the firm, as its CEO, Dan Doctoroff, explained in a 2016 talk, to “target ads to people in proximity, and then obviously over time track them through things like beacons and location services as well as their browsing activity.” One software developer for an Internet of Things company told Zuboff, “We are learning how to write the music, and then we let the music make them dance.”

Such aspirations imply a radical inequality of power between the people who control the play list and the people who dance to it. In the last third of her book, Zuboff takes her analysis up a level, identifying the theoretical ideas and general model of society that she sees as implicit in surveillance capitalism. The animating idea behind surveillance capitalism, Zuboff says, is that of the psychologist B. F. Skinner, who regarded the belief in human freedom as an illusion standing in the way of a more harmonious, controlled world. Now, in Zuboff’s view, the technology industry is developing the means of behavior modification to carry out Skinner’s program.

The emerging system of domination, Zuboff cautions, is not totalitarian; it has no need for violence and no interest in ideological conformity. Instead, it is what she calls “instrumentarian”—it uses everyday surveillance and actuation to channel people in directions preferred by those in control. As an example, she describes China’s efforts to introduce a social credit system that scores individuals by their behavior, their friends, and other aspects of their lives and then uses this score to determine each individual’s access to services and privileges. The Chinese system fuses instrumentarian power and the state (and it is interested in political conformity), but its emerging American counterpart may fuse instrumentarian power and the market.

## **NO FUTURE?**

---

*The Age of Surveillance Capitalism* is a powerful and passionate book, the product of a deep immersion in both technology and business that is also informed by an understanding of history and a commitment to human freedom. Zuboff seems, however, unable to resist the most dire, over-the-top formulations of her argument. She writes, for example, that the industry has gone “from automating information flows about you to automating you.” An instrumentarian system of behavior modification, she says, is not just a possibility but an inevitability, driven by surveillance capitalism’s own internal logic: “Just as industrial capitalism was driven to the continuous intensification of the means of production, so surveillance capitalists are . . . now locked in a cycle of continuous intensification of the means of behavioral modification.”

As a warning, Zuboff’s argument deserves to be heard, but Americans are far from mere puppets in the hands of Silicon Valley. The puzzle here is that Zuboff rejects a rhetoric of “inevitabilism”—“the dictatorship of no alternatives”—but her book gives little basis for thinking we can avoid the new technologies of control, and she has little to say about specific alternatives herself. Prophecy you will find here; policy, not so much. She rightly argues that breaking up the big technology companies would not resolve the problems she raises, although antitrust action may well be justified for other reasons. Some reformers have suggested creating an entirely new regulatory structure to deal with the power of digital platforms and improve “algorithmic accountability”—that is, identifying and remedying the harms from algorithms. But all of that lies outside this book.

| Americans are far from mere puppets in the hands of Silicon Valley.

The more power major technology platforms exercise over politics and society, the more opposition they will provoke—not only in the United States but also around the world. The global reach of American surveillance capitalism may be only a temporary phase. Nationalism is on the march today, and the technology industry is in its path: countries that want to chart their own destiny will not continue to allow U.S. companies to control their platforms for communication and politics.

The competition of rival firms and political systems may also complicate any efforts to reform the technology industry in the United States. Would it be a good thing, for example, to heavily regulate major U.S. technology firms if their Chinese rivals gained as a result? The U.S. companies at least profess liberal democratic values. The trick is passing laws to hold them to these values. If Zuboff’s book helps awaken a countermovement to achieve that result, we may yet be able to avoid the dark future she sees being born today.