ChangeThis

226.03

POLICY IN THE DIGITAL AGE

Michael Lenox

There was a time when Facebook was going to save the world.

In January of 2011, a group of dissidents in Egypt began using Facebook to organize protests against the current government and its leadership. Their efforts soon ballooned into a massive protest movement spreading across the Middle East. All the while, relatively new social media applications such as Facebook and Twitter had become critical to organizing protests, building support within countries, and communicating with the broader world.

With each post, tweet, and YouTube video highlighting the brutal response of the Egyptian government to the protests, global sentiment turned in favor of the protesters. On February 11, the president of Egypt, Hosni Mubarak, resigned.

In the immediate aftermath of the Arab Spring, Time magazine declared "the Protestor" its 2011 person of the year. Facebook and Twitter were cited as transformational technologies that would return power to the people, help encourage governmental transparency, and usher in a new era of freedom and liberty. Some even referred to the events of that spring as the "Facebook revolution." Silicon Valley and its culture of innovation were providing the tools and technologies to transform society for the better. Digital companies were not just building the world's next great products and solutions, they were solving the world's most vexing problems. The digital age was going to be our savior.

Just as the Arab Spring failed to deliver vibrant free societies, digital technology soon found itself the subject of scorn, not celebration. Facebook's moment in the sun quickly faded.

Researchers were finding evidence that social media was creating unhealthy social comparisons, especially among teens and young adults. Some accused Facebook of enabling self-harm and even suicide. Users were finding Facebook to be a forum for the most outrageous of claims and the most vitriolic of comments. CEO and founder Mark Zuckerberg was hauled in front of the US Congress to explain Facebook's algorithms for prioritizing content and to explain how it planned to remove untruthful and harmful posts.

Criticism did not end there. Data privacy, employee health and wellness, use of facial recognition technology, tax avoidance, participation in governance surveillance programs, and censorship policy, among others, had become flashpoints for the company.

Facebook was not alone. All the large technology companies found themselves under greater scrutiny. Google for antitrust and data privacy. Apple for exploiting partners in its App Store. Amazon for its labor practices in both its fulfillment centers and corporate offices. Uber for a toxic work environment that fostered sexual harassment. DoorDash for its refusal to treat drivers as employees. WeWork for overhyping its business results. Airbnb for potential risks to clients from unscrupulous and even predatory renters. The list goes on and on.

For each of the companies cited above, I could cite a dozen other complaints levied on them. Each of these challenges highlight that the digital age is not without peril. Some of these challenges reflect bad management practice and unethical behavior found unfortunately in any age. Some, however, reflect specific issues that are, at the very least, more acute in the digital age. Any company operating in the digital age must understand, account for, and act upon these issues if it is going to flourish.

Complaints are coming from a diverse set of stakeholders. Customers concerned about their personal and digital security. Employees and partners worried about being exploited. Activists looking to advance their specific causes by highlighting the behavior of individual organizations. A news media eager to expose and amplify any concerns. Elected officials responding to their constituencies and, perhaps on occasion, looking to make a name for themselves in the broader public arena. Regulators and other public officials trying to make sense of the applicability of existing rules to the digital arena. Even investors who are growing concerned with the environmental and social performance of companies in which they invest.

For the manager, each of these stakeholders presents risks and opportunities, as important if not more important as what is typically viewed as normal business risk. Like all risks, these "nonmarket" risks need to be understood and managed.

Among the many perils of digitization, perhaps most important is what some are calling the end of privacy.

We say “nonmarket” to highlight that they are often thought of arising in arenas outside the daily operation of business, such as risks arising from activists or policy. However, the term is misleading because these risks are simply the norm when conducting business in the digital age. Your digital strategy would be incomplete if it did not account for and address these nonmarket forces. Thoughtful CEOs know this and actively manage their broader “nonmarket” strategy.

THE END OF PRIVACY

Among the many perils of digitization, perhaps most important is what some are calling the end of privacy. Central to most of the strategies of digital transformation is the acquisition and analysis of data that allows for the creation of value-added services.

On the surface, this need not be problematic. A company using sensors to monitor manufacturing equipment to identify maintenance issues and to help improve production efficiency is unlikely to prove controversial. However, when data comes from individual users and is used to reveal individual preferences and behavior, issues of data privacy become paramount.

What are, and are not, proper applications of user data is a hotly debated topic. On one side, user data can help with the customization of products and services to a user’s specific wants and desires. Think of Spotify’s custom playlists based on your demonstrated listening preferences. To many, even a targeted ad for a new dress on Instagram is not an inconvenience but a delight.

On the other side, of course, are the many ways that user data can be misused. One widely spread story tells of a father who was furious at Target for sending pregnancy ads to his teenage daughter, until it was revealed that the store's algorithm had accurately predicted her pregnancy. More insidious stories abound of employees listening to and sharing private recordings from smart speaker systems.

For companies such as Google and Facebook, user data is central to their business model of selling targeted advertisements to run on otherwise free services. Efforts to give users the ability to control what data is collected and stored by these companies can have a direct impact on the efficacy of the advertisements they provide, lowering the attractiveness of these platforms to advertisers and ultimately affecting the price and demand for advertising on these sites.

This has given rise to what Harvard Business School professor Shoshana Zuboff refers to as "surveillance capitalism," which she defines as

> ***"the unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets–business customers with a commercial interest in knowing what we will do now, soon, and later. An insatiable appetite for user data to make better predictions of their behavior."***

Zuboff highlights that surveillance capitalism is not only about making passive predictions on user behavior, but increasingly about finding ways to shape and direct user behavior.

The big tech companies have hired scores of psychologists and behavior economists to experiment with "nudges"—subtle interventions desired to shape your behavior. While sometimes those nudges can be towards arguably desirable ends—reminding you to save money for retirement or motivating you to work out—they can also be used to influence what you buy and shape your preferences.

This was never more evident than in the 2016 US presidential election, when it was discovered that foreign actors were purposefully sowing discord on online platforms such as Facebook and Twitter and even trying to incite citizens to take to the streets and engage in violent protest.

Surveillance capitalism is not an unavoidable outcome of digital technologies. It is a choice by businesses. For a business, it derives from the choice of a business model predicated on exploiting user data. Often policymakers are complicit, allowing businesses to pursue such strategies and failing to provide safeguards that allow users to truly own their data.

It doesn't have to be that way.

Of course, even when a company promises to keep your data private, there is the question of how protected your data is from cybersecurity threats.

Consider Apple. Apple's business model is largely to sell hardware devices to customers. This helps mitigate some of the demand for exploitation of user data. Apple can use your data to improve the products it provides to you while also promising you a certain degree of protection for your data, such as shielding it from other parties. It can empower data owners.

This tension between business models came to a head in April 2021 when Apple allowed its users to easily opt out of data tracking by applications as you use your mobile device. Over 96 percent of Apple iPhone users opted out of such tracking. This has had a large material impact on companies such as Facebook, which forecasted a $10 billion decline in 2022 advertising revenue because of the change in Apple's data policy.

Of course, even when a company promises to keep your data private, there is the question of how protected your data is from cybersecurity threats.

In 2013, Target was hit with a massive cyberattack that compromised forty million customers' credit and debit card numbers. In an analysis of what happened, it was determined the malware that perpetrated the attack entered Target's systems through a personal computer attached to the HVAC system at one of its facilities by an unaware air conditioner repairman. Within hours, the malware had moved through the HVAC system and into the company's servers, ultimately infiltrating the cash registers in its network of stores.

A massive shadow industry of illicit hacking now spans the globe. Supported by the dark web and cryptocurrency, the hacking market has evolved into a sophisticated international exchange.

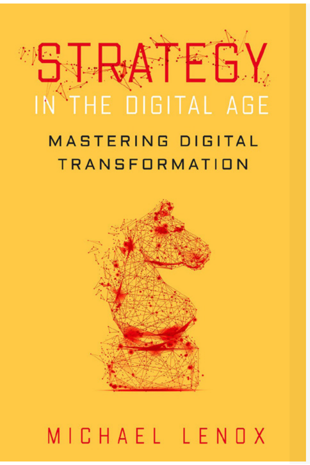
Some estimates put the money collected worldwide from ransomware at $18 billion, nearly $350 million in the United States alone. Global crime syndicates have been found to deploy sophisticated cyberattacks against companies and governments around the world. Some of these hacker groups, with names like DarkSide and REvil, are selling their services to the highest bidders.

Of course, the most severe privacy risks may still come from within the organization. Sensitive health information could be misused by employers. Facial recognition could be used to track the movement of customers and employees without their knowledge or consent. These concerns have become particularly pronounced as these technologies have moved into the public arena, adopted by governments and police departments. In the United States and abroad, we are seeing the increased use of facial recognition and other data-driven techniques to try to identify and track criminals.

"When does the right to privacy begin and when does it end?" is a question all organizations will have to grapple with in the digital age.

Adapted from *Strategy in the Digital Age: Mastering Digital Transformation,* published by Stanford Business Books.

Info



Ready to dig deeper into the book?

Buy a copy of Strategy in the Digital Age.

Want copies for your organization or for an event?
We can help: customerservice@porchlightbooks.com
800-236-7323

ABOUT THE AUTHOR

Michael Lenox is the Tayloe Murphy Professor of Business Administration at the University of Virginia's Darden School of Business. He is the coauthor of *Can Business Save the Earth? Innovating Our Way to Sustainability* (Stanford, 2018) and *The Strategist's Toolkit* (Darden, 2013).

SHARE THIS

Pass along a copy of this manifesto to others.

SUBSCRIBE

Sign up for e-news to learn when our latest manifestos are available.

Curated and edited by the people of Porchlight, ChangeThis is a vehicle for big ideas to spread. Keep up with the latest book releases and ideas at porchlightbooks.com.

This document was created on July 19, 2023 and is based on the best information available at that time.