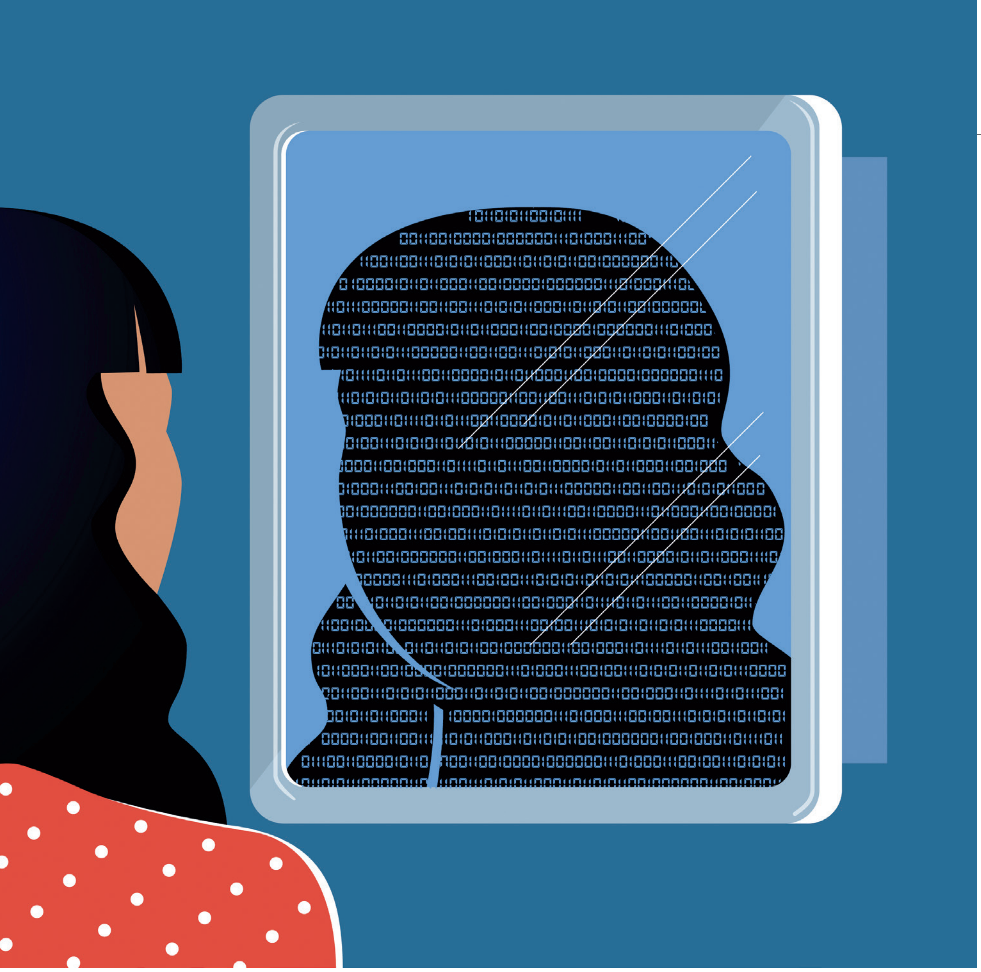

Our Data, Ourselves

How to stop tech firms from monopolizing our personal information.

By Philip N. Howard

C**ONCENTRATED IN A FEW HANDS,** big data is a threat to democracy. Social media companies and political data-mining firms such as Cambridge Analytica have built their businesses by manipulating public life using personal data. Their work has helped heighten ethnic tensions, revive nationalism, intensify political conflict, and even produce new political crises in countries around the world—all while weakening public trust in journalism, voting systems, and electoral outcomes.

Such crises are symptoms of a deeper problem: the effective monopoly that a handful of technology firms have gained over a wealth of information relevant to public life. Fixing the situation requires putting the public back in charge of its data.

Democracy has long been predicated on, and reinforced by, social institutions that carefully collect information about public life and collective needs. Today, however, a handful of technology companies have far exceeded the data-gathering capacity of all other kinds of organizations. These private firms possess detailed information on the public—and having collected and stored data on every user's attitudes, aspirations, and behaviors, they then use it to serve their bottom line. Social media platforms are designed to deliberately exploit the common predilection for selective exposure—the tendency to favor information that confirms preexisting views—to reinforce messaging from advertising clients, lobbyists, political campaign managers, and even foreign governments.

There are two ways to protect democracy from the challenge posed by tech companies' dominance over socially valuable data. The first option is for governments to regulate content on an unprecedented scale. That would oblige public regulators to either review all social media content to judge its appropriateness or provide clear signals to private firms—whether the social media companies themselves or third parties—to perform such content reviews. But the problem with both scenarios is that they would create massive new censorship mechanisms that would further threaten democratic culture.

Far preferable would be market regulations that guide firms on how and when they can profit from information about individuals. Such regulations would put the public back in charge of a valuable collective resource while still allowing citizens to express themselves individually by deciding what to do with their data. To get there, policymakers should focus on five basic reforms, all of which would put public institutions back into the flow of data now dominated by private firms.

First, governments should require mandatory reporting about the ultimate beneficiaries of data. That means, when queried, technology firms should be required to clearly report to users which advertisers, data miners, and political consultants have made use of information about them. Your Facebook app or your smart refrigerator should be required to reveal, on request, the list of third parties benefiting from the information the device is collecting. The trail of data should be fully, and clearly, mapped out for users so that if a data-mining firm aggregates users' data and then sells it on to a political party, the users could still identify the ultimate beneficiary.

Second, regulations should require social media platforms to facilitate data donation, empowering users to actively identify the civic groups, political parties, or medical researchers they want to support by sharing their data with them. In freeing data from private actors, governments could create an opportunity for civic expression by allowing citizens to share it with whichever organizations and causes they want to support—not just the ones that can afford to buy it, as is the case today.

The third reform is related to the second: Software and information infrastructure companies should be obliged to tithe for the public good. Ten percent of ads on social media platforms should be reserved for public service announcements, and 10 percent of all user data should be obliged to flow (in a secured way) to public health researchers, civic groups, professional journalists, educators, and public science agencies. Such a system would allow many kinds of advocacy groups and public agencies, beyond Facebook's private clients, to use existing data to understand and find solutions for public problems.

Fourth, the nonprofit rule on data needs to be expanded. Most democracies have rules that prevent firms from profiting from the sale of certain kinds of public data. In many U.S. states, for example, data-mining firms can't profit from the sale of voter registration data, which public agencies collect. This rule needs to be extended to a wider range of socially valuable data, such as places of employment, that is now gathered by technology companies. Such classes of information could then be passed to public agencies, thus creating a broader set of data in the public domain.

Fifth, public agencies should conduct regular audits of social media algorithms and other automated systems that citizens now rely on for information. Technology companies will call these algorithms proprietary, but public agencies currently audit everything from video gambling machines to financial trading algorithms, all in ways that don't violate intellectual property.

Users should have access to clear explanations of the algorithms that determine what news and advertisements they are exposed to, and those explanations should be confirmed by regular public audits. Moreover, all ads, not just political ones, need to be archived for potential use by public investigators. Audits of today's technology would also put the designers of new technologies—such as artificial intelligence—on notice that their own algorithms will one day be under scrutiny.

Little of this need be wishful thinking. Restoring public access to social information wouldn't require legislators to pass a raft of new laws, since most democracies have the public science agencies, libraries, and privacy czars needed to effectively administer large collections of public information. Competition regulators in the European Union and United States may already have the authority to set mandatory guidelines for any technology company with a business model that relies on controlling vast stores of publicly valuable data. Europe's General Data Protection Regulation, which has boldly asserted an individual right to control data since going into effect in May, is an important start. It is already having a global impact, as many technology firms find it easier to implement a platformwide response than to adjust particular features for users based in Europe.

Tech firms might claim that such demands would infringe on their economic rights as private enterprises. But contrary to such suggestions, it's entirely fair to regulate the operations (if not the content) of tech firms because the platforms they control have become the fundamental infrastructure for public life. They are a common carrier for our political culture, much the same way the post office, newspaper empires, and television and radio broadcasters conveyed politics in past decades while being regulated to varying degrees.

In democracies, citizens expect media companies, journalists, and civic groups to have some public duties, often enforced through the law. Social media and data-mining firms have evaded those responsibilities until now, hoarding public data with little public oversight. Strengthening democracy will require putting socially valuable data back to work for the public good. ■

Tech firms might claim that new guidelines would infringe on their economic rights as private enterprises. But it's entirely fair to regulate the operations (if not the content) of tech firms because the platforms they control have become the fundamental infrastructure for public life.

PHILIP N. HOWARD (*@pnhoward*) is a statutory professor of internet studies at the Oxford Internet Institute and Oxford University's Balliol College.