COMMENTSeptember/October 2018 Issue

Data to the People

India's Inclusive Internet

By Nandan Nilekani

https://www.foreignaffairs.com/articles/asia/2018-08-13/data-people

Data, the techno-optimists are fond of saying, is the new oil. It is the fuel of the modern economy, a valuable commodity that can be bought and sold, and a strategic resource for nations. Indeed, digital assets now matter far more than physical ones. As the writer Tom Goodwin has pointed out, "Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate." As with oil in another era, the market today has generously rewarded those who have best captured data. In 2006, three of the world's six most valuable public firms were oil companies, and just one was a technology company. By 2016, only one oil company remained in the top six. The rest were tech giants.

But the oil metaphor has turned out to be inaccurate—not because it overhyped the role of data but because it failed to warn us just how pervasive and problematic our relationship with data would become. The Internet, it has become clear, is not so free, after all; users are paying in the form of personal information, which is collected by "data brokers" and sold to third parties. Earlier this year, news broke that the political consulting firm Cambridge Analytica had harvested personal data from tens of millions of Facebook users and sold it to political campaigns. The scandal showed how malicious actors could wield data to threaten the democratic process, and it led to a congressional hearing featuring an apologetic Mark Zuckerberg, the CEO of Facebook, and prompted broader soul-searching about the power of massive technology companies. At its peak, Standard Oil could influence what people paid for fuel, but today's big technology companies can influence what people think.

The world is beginning to suspect that the basic incentive structure of the Internet itself may be flawed. Many online businesses face a deep underlying conflict between their own interests and those of their users. Just as concerns about unaccountable oil monopolies at the beginning of the twentieth century led to new antitrust measures, concerns today about the growing power of the companies that collect and sell personal data have led to calls for governments to fundamentally rethink their approach to regulating the Internet. As they do so, they cannot afford to ignore the one country leading the way in developing a new model of how citizens relate to the Internet, a place that treats digital infrastructure as a public good and data as something that citizens deserve access to: India.

THE STATE AND THE WEB

Different governments have approached the question of Internet regulation in very different ways. The United States has taken a market-centric approach, with light or no regulations, allowing innovators room to grow rapidly. Consider what *Wired* has called "the most important law in tech": Section 230 of the Communications Decency Act of 1996, which stipulates that online platforms, unlike their analog counterparts, are not liable for the content posted by their users. By exempting Facebook, Google, Twitter, and others from stifling legal and regulatory risks, the provision powered the rapid growth of the U.S. technology industry. But it also absolved those companies of any blame regarding what third parties were doing with users' data.

Europe has taken a more activist approach to Internet regulation, especially when it comes to privacy. In May of this year, the EU's General Data Protection Regulation, or GDPR, went into effect. Before the law, citizens signing up for an online service were required to educate themselves about their rights and what they were consenting to. In a major improvement, the GDPR shifts the burden for privacy and security onto to the service providers. It establishes strict rules governing how firms collect and handle personal data and sets forth steep fines for violations. But it's important to recognize that the GDPR is primarily a legal solution; it can only seek to deter, not prevent, malicious actors from putting their business needs over the interests of the user.

It is in Asia, however, where the future of the Internet is most likely to be written. China and India are the two largest markets for the Internet in the world, with 772 million and 481 million users, respectively. They are also the top two smartphone markets, and together they constitute 39 percent of the world's 830 million youth on the Internet. As developing countries, both are free of the baggage of legacy systems that the Internet had to disrupt. Take the rise of online payments in China: a country that just five years ago still predominantly used cash now sends $9 trillion annually in mobile payments. Americans, who aren't yet as savvy at conducting financial transactions on their phones, send just $49 billion via mobile transfers annually. For the developing world, digital technologies represent a palette of possibilities on a blank state.

The future of the Internet is most likely to be written in Asia.

Although both China and India understood that the Internet would have a huge impact on their economies, they have charted two very different courses for regulating it. China sees the Internet as something to be controlled and censored. Under the banner of "cyber-sovereignty," the government has attempted to keep Chinese cyberspace cordoned off from the larger Web and to control the information available to its citizens. Famously, it has built "the Great Firewall," which blocks access to foreign websites and platforms. But because there are cracks in the wall—foolproof controls are difficult for any government to impose—China also relies on the cooperation of private companies, which show little resistance to sharing data with the government. Alibaba and WeChat are competing to provide a digital version of China's national identity card, required for everything from opening a bank account to getting a driver's license. Chinese firms have even begun participating in the government's "social credit" system, whereby people are rewarded for good behavior, such as conserving energy, and penalized for bad behavior, such as spreading online rumors.

Chinese officials claim that their objective isn't simply to protect personal information but to protect national security, too. Accordingly, this past January, the government announced new national standards on the protection of personal information that, compared with the GDPR, cover more types of data and require more stringent security precautions. The rules also mandate that certain data must remain inside China's borders at all times, so that the government has jurisdiction over its use.

It is easy to dismiss the Chinese approach as authoritarian. And indeed, the government has used its control to stifle discontent. But Beijing can rightly assert that it has created local competition for Big Tech. China is the only country to create rivals that match the size of the U.S. tech giants, with the homegrown companies Alibaba, Baidu, and Tencent. Beijing can also point out that it is managing to restrict some of the bad effects of the data economy: for example, thanks to the government's constant monitoring of content, outsiders would have an extremely hard time influencing politics in China. This heavy-handed approach may or may not work, but many nations will look to China's model as they seek to control cyberspace in their own countries.

India believes the solution lies in a different approach. Instead of seeking to exert tighter control over the Internet within its borders, the country has created open digital platforms from scratch and tailored them to the Indian context. And instead of leaving them in the hands of a few private technology companies, the Indian government has built these systems as public goods.

IDENTITY FOR ALL

This approach was pioneered in 2009, when India decided to establish a national identity system. Back then, the system for distributing subsidies, largely run on paper and documented in handwritten ledgers, was rife with corruption. A major upgrade was needed; merely replacing ledgers with spreadsheets wasn't going to work. The root problem was the lack of a trustworthy identity for every resident. If everyone had a trustworthy identity, the thinking went, people would have an easier time opening bank accounts, obtaining credit, and enrolling in social welfare programs.

Thus was born Aadhaar, the world's largest biometric ID project, a government program that I headed until 2014. Those who sign up for an Aadhaar number—a unique, randomly generated string of 12 digits—must have their faces photographed, their fingerprints taken, and their irises scanned. That ensures that there are no duplicates or fakes, creating a highly trustworthy database. The system also includes a publicly available interface, or open API, which allows any licensed service provider to verify if users are who they claim to be. People can use Aadhaar to open bank accounts, buy SIM cards, receive entitlements from the government, sign forms electronically, invest in mutual funds, get credit, rent bicycles, and more.

Aadhaar exemplifies India's commitment to the notion that digital infrastructure should be a public good.

Aadhaar, whose name translates as "foundation" in Hindi and other Indian languages, was the first "foundational ID" issued by the government of India. Unlike a driver's license or a passport, foundational IDs come with no specified purpose or attached entitlement. Aadhaar numbers have no defined function, and simply getting one doesn't automatically make a person eligible for any subsidy. Anyone and everyone who is a resident of India can get an Aadhaar number, and it lets a person prove just one fact: "I am me."

Aadhaar has become the foundation of a host of transformative projects within the government. In 2014, the government launched the Prime Minister's People's Wealth Scheme, which gives low-cost, no-frills bank accounts to the underserved, provided they can supply details about their identity. From 2014 to 2017, the number of simple bank accounts such as these in the country grew tenfold, from 30 million to 300 million, thanks partly to the availability of Aadhaar authentication. Another program, the Direct Benefit Transfer, allows the federal government to place subsidies—scholarships, money for fuel, pensions, and so on—directly into the bank accounts of poor Indians, rather than go through numerous middlemen, who invariably take their own cut. Because a recipient can tie his bank account to his Aadhaar number, the government can be sure that it has sent money to a unique individual just once, thus eliminating the problem of double dipping and other forms of corruption.

Within five and a half years after its launch in 2009, Aadhaar had reached one billion users—an especially impressive achievement given that enrollment requires biometric registration. Today, it has 1.21 billion enrollees and counting, and every month, it processes around one billion authentications. Since Aadhaar's inception, the government has sent payments from 432 different benefit schemes totaling over $57 billion through 3.2 billion direct transfers, saving the government $13 billion. More than 500 million unique people have had their identities authenticated through the open API at least once.

Aadhaar is not a silver bullet, however. Critics have pointed out that some people have a harder time proving their identity. Manual laborers, for example, often have calloused hands that fingerprint scanners are unable to read reliably. There are technological solutions to this problem, such as relying on Aadhaar's iris scanning or face identification function to verify an identity in lieu of fingerprints, but there often isn't the expertise to use it. So the real solution is to invest in training and manpower so that these cases can be dealt with on the ground.

Aadhaar has also come under fire for threatening privacy. Critics have arguedthat a single identification number, by its very existence, threatens the privacy of those who hold it, because it allegedly gives the state the ability to profile and surveil them. Earlier this year, the Supreme Court of India began presiding over a landmark case to decide if this argument holds any merit. Here again, technology can help ameliorate the problem, but the real threat to Indians' privacy comes in spite of Aadhaar, not because of it. India desperately needs to put in place a law that protects its citizens from the wrongful use of their personal data. And because the average Indian is apathetic about the protection of personal data, India needs to do more to make its people aware of the rights they do have.

DIGITAL PUBLIC GOODS

Aadhaar exemplifies India's commitment to the notion that digital infrastructure should be a public good. That is not how much of the world's digital infrastructure is conceived of. Online identity forms the foundation of trust for all the services people use on the Internet, yet for now, the two biggest providers of identity are private tech giants: Facebook and Google. What makes those companies so powerful is their ability to aggregate data and link it to individual identities. They know not just users' demographic details but also their behavior. This information enables Internet platforms to show people more relevant ads and content, but it can also be weaponized, as the Cambridge Analytica scandal has shown.

Aadhaar, by contrast, was built as a public good and paid for by the government, and so there was no need to construct deeper profiles in pursuit of advertising revenue. In many respects, it is a "dumb" ID, capturing less information about users rather than more. It knows only four data points about each holder: name, date of birth, address, and gender. Aadhaar incorporates privacy into its design in other ways, too. When a service provider sends an authentication request to Aadhaar, the purpose of the authentication is not revealed; all the government knows is when someone uses his Aadhaar number, not where or why. Another feature generates a "virtual ID," a temporary number that links to one's Aadhaar number and can be used to verify one's identity yet can be shared without worrying about data brokers creating a detailed individual profile by gathering one's information from disparate databases.

> *Regulating Big Tech is not going to be a purely legal affair. The Internet is still unfinished.*

Aadhaar marked the first time the Indian government stepped up to create digital infrastructure as a public good, but not the last. The government has built a collection of nationwide digital platforms, known as "India Stack," that allow government agencies and businesses to safely serve a billion-plus Indians in real time and at a low cost. In 2012, to increase access to financial services, the government launched a system through which Indians could easily complete the "know your customer," or KYC, requirements that businesses such as banks and telecommunications companies use to assess potential clients and comply with regulations. The program, called e-KYC, lets users complete the process paperlessly, dramatically cutting the costs for businesses to sign up new customers. In 2017 alone, 3.4 billion e-KYC processes were completed. The result: Indians have greater and more affordable access to financial products such as credit, insurance, and mutual funds.

Another part of India Stack is the Unified Payments Interface, launched in 2016. Just as the SMS protocol allows users to send a text message from an iPhone on one network to an Android phone on another, UPI lets them seamlessly send money between various banks and financial service providers. Since the platform is a public good, any bank can make UPI a part of its mobile app with just a few lines of code. It also enhances competition and consumer choice. Because UPI is fully interoperable, Indians can now conduct transactions on their State Bank of India account from inside the Citibank app. The costs of switching between banks are dramatically lowered, so banks must compete for customers' business. Not surprisingly, UPI is proving popular: in June 2018, the platform handled 246 million transactions (more than the average number of monthly credit card transactions in India), totaling some $4billion. And now that the messaging app WhatsApp has integrated UPI into its system, its 200 million Indian users can send money easily through an interface they already know and trust.

DATA IS POWER

If the idea that digital infrastructure should be a public good is the first guiding principle of the Indian approach to the Internet, the second is that people should be empowered by data. As the Peruvian economist Hernando de Soto has argued, those who are left out of the formal economy—for example, small-scale entrepreneurs with no bank accounts—suffer from being excluded. Enabling them to have a trustworthy digital identity is one way to bring them into the formal economy. Once they have that, they benefit not only in the expected ways, such as by having an easier time opening a bank account, but also in a more subtle way: they can start generating their own data. As more and more parts of Indians' lives go online, more and more data will be produced. In fact, given the glut of data that will be generated from their smartphones, smart cities, and other physical devices connected to the Internet, it is fair to say that Indians will be data rich before they become economically rich.

How can this data wealth be turned into actual wealth? The question highlights the prickly problems around data. To benefit from data, one must be able to access it and assert ownership over it. With the advent of three-party or even four-party data transactions—such as a purchase between a buyer and a seller that takes place through an online marketplace—the issue of ownership is still unclear. But across the globe, there is a growing consensus when it comes to access: users must be allowed to obtain their data and use it any way they see fit.

India has operationalized this principle through two important initiatives. The first is the voluntary standard that the Ministry of Electronics and Information Technology has encouraged organizations to use to gain users' consent to share their data. Under this system, users digitally sign an electronic document that specifies who can use the data, for how long, and whether the information can be shared further. Unlike obfuscatory privacy policies, this contract sheds all ambiguity by standardizing and codifying the purpose of data use. And because the agreement is enshrined in computer code, users have the ability to revoke consent: with a simple click, a user can choose to stop providing services with data.

Enrolling villagers for Aadhaar in Rajasthan, India, February 2013.

The second initiative is the concept of "data fiduciaries," a type of organization being envisioned in India. A data fiduciary can be thought of as a personal consent manager. Its purpose is to ensure that any transaction that requires sharing one's data happens in a safe and consensual manner. Ideally, it would be legally bound to prioritize the interests of the person who is handing over the data, and not those of the entity requesting it.

The first incarnation of a data fiduciary is the "account aggregator," an entity for which the Reserve Bank of India issued guidelines in 2016. Account aggregators collect customers' financial data and share it with their consent. In the past, it was tremendously hard for an Indian to get a statement of his bank account; when applying for a loan, he had to share either verified paper records or his banking password with the lender, not knowing what data might be extracted. With account aggregators, customers can allow certain financial data to be shared safely. And because the account aggregators operate on a fee-for-transaction business model and are legally prohibited from storing or selling data, users can rest assured that their privacy is respected.

Other data fiduciaries that are in the works now will allow job seekers to prove their credentials and employment history, which should empower them to demand better wages befitting their experience. Data fiduciaries are also being developed in India's healthcare sector, to allow patients to control who can access their health records.

A MODEL FOR ALL

India's approach to the Internet is simple: empower users with the technical and legal tools required to take back control of their data. In practice, this has meant investing in digital infrastructure that is open and interoperable, thus enabling billions of low-cost, high-trust transactions. Although this model was designed for and by Indians, it can be applied anywhere.

Indeed, the rest of the world is starting to take notice, with some 20 countries now looking to build their own versions of India Stack, including Afghanistan, Bangladesh, Morocco, the Philippines, Rwanda, and Singapore. Earlier this year, the philanthropist Bill Gates encouraged other countries to build their own versions of Aadhaar, and his foundation is funding efforts by the World Bank to, in his words, "take this Aadhaar approach to other countries." That is a wise investment, since building such digital infrastructure is a relatively low-cost endeavor: it cost only about $1 per resident to give almost everyone in India an Aadhaar card, and it has paid for itself many times over thanks to savings through the Direct Benefit Transfer. Creating digital infrastructure as a public good has the added benefit of making it subject to public oversight. Instead of trusting private companies to collect and use people's data responsibly, countries can design the system with checks and balances already in place.

India's approach need not be confined to India. Indeed, it was hardly the first country to view digital infrastructure as a public good. The Internet itself was born out of ARPANET, a project funded by the U.S. Department of Defense that began in 1969. Likewise, GPS was developed for the U.S. military but opened up to civilian use in the 1980s. But over time, the private sector created newer platforms on top of these public goods. While many of these private platforms were still available for anyone to use, they were often built as walled gardens rather than open playgrounds.

What other countries should realize is that regulating Big Tech is not going to be a purely legal affair. The Internet is still unfinished. Like India, countries that believe in openness—such as the United States and European states—should participate in the shaping of the Internet itself. Rather than merely passing laws, they should help create platforms, ratify standards, and design fiduciary institutions to ensure that privacy, competition, and interoperability are baked into technology instead of being tacked on as an afterthought.

For too long, governments have held an overly limited conception of their role regarding the Internet, seeing their job as merely facilitating citizens' access and letting private players handle the rest. But India's example shows that there is a better way: ensuring that citizens get access to a fair and open Internet and empowering them with their data.