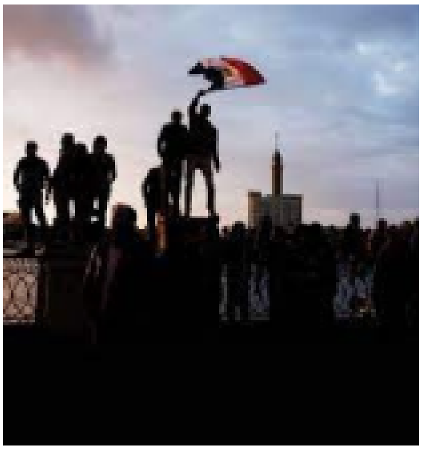
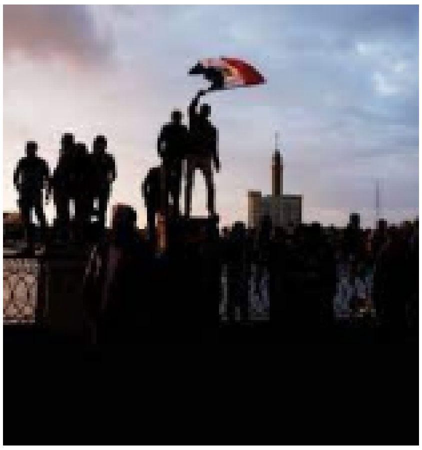
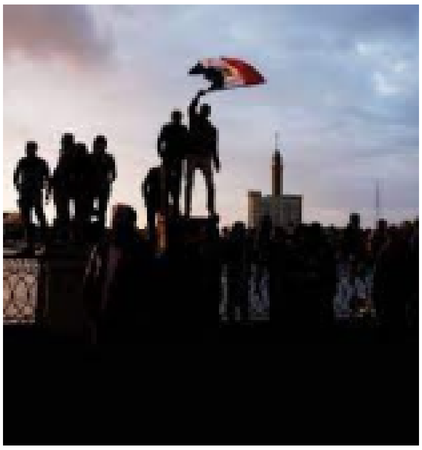
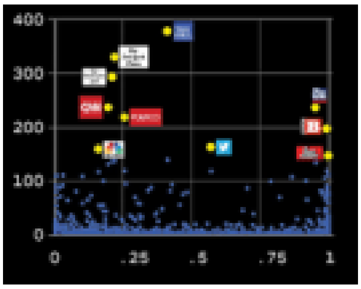


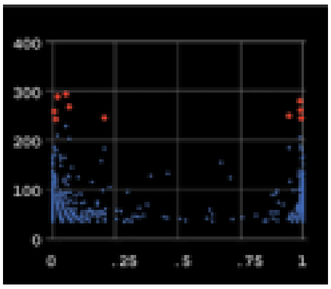




A press divided

If social media were merely a distraction from an otherwise normal diet of professional news, its impact on democracy would be limited. But this map from scholars at Harvard's Berkman Klein Center and MIT's Media Lab, based on "co citations" (i.e.. who links to whom), shows that the media world is bifurcated too


400
300
200
100
0
0
.25
.5
.75
1


400
300
200
100
0
0
.25
.5
.75
1

@Jenn_Abrams

Mainstream
liberal

DC journalists

Activisit right

T

31From 2008 to 2020

2018

This year, campaigns will again deploy a broad range of technological tools to find and communicate with voters, using what they know about them to person alize ads, calls to volunteer and vote, and requests to donate. But the targeting is becoming ever more effective as more data on voters becomes available and tools for using it get better and more numerous.

The Democratic National Committee has set up a marketplace of vendors for the party's candidates. Left leaning Higher Ground Labs has a portfolio of incubated startups offering polling, cheaper advertising "persuasion science," and fund-raising tools like CallTime.ai, which tries to apply artificial intelligence to attracting donations. On the right-leaning Lincoln Network's app marketplace, many of the same vendors, from Salesforce to the community-management platform Nationbuilder, are avail- able to conservative campaigns.

While the main factor in the midterms will be the voters' judgments on the Trump administration, smart uses of technology could make a difference in tight races. The tools available allow political novices to quickly gain direct access to attention and fund- raising if their candidacies and messages resonate with people even if they are ignored by media outlets. Alexandria Ocasio-Cortez, a 28-year-old com- munity activist, unseated a 20- in New York's Democratic pri- mary for Congress, thanks in part to her viral video.

After the Russian "dark ads" and Cambridge Analytica scandals, will online campaigning at least be less murky? Yes, but not by much. Twitter and Facebook have made political ads more transparent, enabling the public to see who has bought them and putting advertisers through a vetting process; Google is expected to follow suit. But true transparency would mean having a file of all paid political ads, on a public website, with bulk open data downloads and an application programming interface (API) so that people could get the data without having to log into Twitter or Facebook themselves. It would also be backed up by a law instead of being volun- tary. (Disclosure: I have a position on this, since while at the Sunlight Foundation I helped senators draft the Honest Ads Act. If enacted, the bill would not only mandate disclosures and disclaimers but update the definition of electioneering to include online platforms.)

In any case, these moves address only a tiny part of the problem. Political organizations and foreign states have long been able to channel "dark money" into political campaigns through nonprofits with out identifying the source, and in July of this year, the US Treasury relaxed those rules even further. Regulating ads on social media also wouldn't address disinformation by foreign states or reverse the various Supreme Court decisions that have weakened US campaign-finance laws over the past decade.

2020 and beyond

Expect the campaigns in the next presidential race to use not radically new sorts of tools but more of the same: more data, better algorithms, and, consequently, more fine-grained targeting of voters, especially those judged to be crucial to tipping a district or a state in a candidate's favor.

What will probably evolve faster are the ways messages to those voters are created and spread. There may be gimmicks such as virtual-reality town-hall meetings or geotargeting-sending voters ads on their phones when they're near polling places or campaign events, for example. But the technology that's likely to have the most impact is something seemingly less advanced: video.

Many more people now have good enough mobile broadband to stream high-quality video on their phones than did just a few years ago. That's part of why unknown candidates on small budgets, such as Ocasio Cortez, can become overnight sensations. As mobile video becomes more popular, though, it's also going to be exploited more as a tool of misinformation. Readily available software for creating video "deepfakes," such as the head of one person digitally swapped onto the body of another, is rapidly improving (see "Fake America great again," page 36). Generative adversarial networks (GANs), Al tools that pit two algorithms against each other, can be used to auto- mate the creation of entirely artificial but believable imagery from scratch.

If the 2016 presidential race brought "fake news" into the lexicon, in 2020 the struggle to distinguish it from reality will reach a new level. For companies like Facebook, already under siege for permitting conspiracies and hate speech to circulate on their platforms, this may finally force a reckoning with society- and with legislators and regulators-about their responsibility, as the world's largest purveyors of information, to prevent the spread of personali-zed disinformation.

Alex Howard is a wiiter and open-government advocatebased in Washington, DC, and former deputy director of the Sunlight Foundation.

The events of 2016 shattered the worldview of the internet idealists. Now they are casting around for alternatives.

By **Tim Hwang**

A field guide to the depressed former internet optimists

A long time ago, in the bad old days of the 2000s, debates about the internet were dominated by two great tribes: the Optimists and the Pessimists.

"The internet is inherently democratizing," argued the Optimists. "It empowers individuals and self-organizing communities against a moribund establishment."

"Wrong!" shouted the Pessimists. "The internet facilitates surveillance and control. It serves to empower only governments, giant corporations, and on occasion an unruly, destructive mob."

These battles went on at length and were invariably inconclusive.

Nevertheless, the events of 2016 seem to have finally shattered the Optimist consensus. Long-standing con cerns about the internet, from its ineffectual protections against harassment to the anonymity in which teenage trolls and Russrelief against the backdrop of the US presi dential election. Even boosters now seem to implicitly accept the assumption (accurate or not) that the internet is the root of multiple woes, from increasing political polarization to the mass diffusion of misinformation.

Tim Hwang is director of the Ethics and Governance of AI Initiative, a joint program of the MIT Media Lab and Harvard's Berkman Klein Center. (He is not to be confused with Tim Hwang, CEO of FiscalNote, profiled on page 56.)

All this has given rise to a new breed: the Depressed Former Internet Optimist (DFIO). Everything from public apologies by figures in the technology industry to informal chatter in conference hallways suggests it's become very hard to find an internet Optimist in the old, classic vein. There are now only Optimists-in-retreat, Optimists in doubt, or Optimists-hedging-their-bets. As Yuri Slezkine argues wonderfully in The House of Government, there is a process that happens among believers everywhere, from Christian sects to the elites of the Russian Revolution, when a vision is unexpectedly deferred. Ideologues are forced to advance a theory to explain why the events they prophe sied have failed to come to pass, and to justify a continued belief in the possibility of something better.

Among the DFIOs, this process is giv ing rise to a boomlet of distinct cliques with distinct views about how the inter net went wrong and what to do about it. As an anxiety-ridden DFIO myself, I've been morbidly cataloguing these strains of thinking and have identified four main groups: the Purists, the Disillusioned, the Hopeful, and the Revisionists.

These are not mutually exclusive posi tions, and most DFIOs I know combine elements from them all. I, for instance, would call myself Hopeful Revisionits.

The question is, do these tribes matter? Or are the Pessimists ultimately right that the internet is essentially destructive to soci ety?

I say no. Both Optimism and Pessimism make the mistake of assuming that the internet has inherent features, but like any technology conceived of and built by humans, it is shaped by human struggles, by the push and pull of a multitude of inter- ests and schools of thought. one that celebrates what's working, is hon est about what isn't, and articulates a path forward grounded not so much in techno logical fixes as in a richer understanding of trust, identity, and community.

The political wstem compensated for a lack of data on individual activities by deterring dissent broadly and harshly.

Big data would be a threat if Chinese citizens could be expected to have an abundance of political and civil liberties in its absence. But China is a repressive, authoritarian society with or without big data.Technology has made the repression more precise, but precise repression might be an improvement over indiscriminate repression.

Traffic is expensive

In a segment on The Late Show earlier this year,comedian Stephen Colbert told his audience that the social credit scores being rolled out in China would dock citizens for instances of jaywalk ing, among other things. That might sound harsh, but then Colbert has evidently never driven in Beijing.

Alibaba, China's largest online retailer, is using cloud computing to combat China's suffocating traffic. In 2016, the company introduced a traffic management system called City Brain in Hangzhou, where Alibaba is headquartered. Unlike Google Maps for video footage of traffic incidents. The municipal government relies on City Brain where Alibaba is

headquartered. Unlike Google Maps for video footage of traffic incidents.

China is a repressive society with or without big data.Technology has made the repression more precise,but that might be an improvement over indiscriminate repression.

Better or worse than what?

China's surveillance culture existed long before the rise of big data. In his book The Government Next Door, Luigi Tomba details how Chinese politics have been micromanaged at the neighborhood level. Residential communities are monitored by neighborhood committees performing semigovernmental functions: reporting dissent, resolving conflicts, and managing both petitions to the government and pro tests against it. These functions used to be the task of retired elderly women, whom the former Wall Street Journal reporter Adi Ignatius memorably called the "small-feet KGB." (In traditional China, women had their feet bound at birth.) The question is whether monitoring and repression tj rough impersonal technology is better or worse than these personal intrusions.

One of the most important roles of the small-feet KGB was to enforce China's one-child policy. The Chinese fertility rate fell dramatically while the policy applied, from 1979 to 2015-a testament to the effectiveness of these personal surveillance tactics.

In ancient China, there was a joint liability system under which three to five households were linked together. If a member of one household committed an offense, all the households were punished. During the Cultural out to their immediate family members.

The municipal government relies on City Brain to identify the best routes for emergency vehicles and to plan new roads and bus routes.

Might City Brain also be used for some Big Brothersh functions? Probably, but ne easing China's traffic nightmares and get ting emergency patients to the hospital and getting emergency patients to the hospital About 20 percent of the gasoline consumed in China is wasted.

The social benefits gained through big- g data technology don't obviate the political downsides. The question is: just how d "down" is the downside, and how "up" is s. the upside?

Cyberattacks on the 2016 US election caused states to bolster the defenses of their voting systems. It hasn't been enough.

By Martin Giles
Portrait by Lyndon French

Your vote is in jeopardy

Russian hackers targeted US elec toral systems during the 2016 presi dential election. Much has been done since then to bolster those systems. but J. Alex Halderman, director of the University of Michigan's Center for Computer Security and Society, says they are still worryingly vulnerable (see "How hackers could cause chaos," page 46). MIT Technology Review's Martin Giles discussed election security with Halderman, who has testified about it before Congress and evaluated voting systems in the US, Estonia, India, and e lsewhere.

Lots of things, from gerrymandering to voter ID disputes, could undermine the integrity of the US electoral process. How big an issue is hacking in comparison?

Things like gerrymandering are a question of political squabbling within the rules of the game for American democracy. That's not playing by the rules of American politics; that's an attempt to subvert the foundations of our democracy.

How much has election security improved since the 2016 US presidential election?

One thing that's improved is awareness. States are taking the first necessary steps to protect their systems-things like making sure they run vulnerability scans on software, and that electoral staff have security clearance to receive threat intelligence from the federal government. Progress accelerated in March when Congress allocated $380 million in new funding that will help states afford to upgrade insecure equipment and make other improvements, but there's still a lot more work to be done.

What element of the voting process worries you the most?

The part that keeps me up at night is t he electronic voting machines. Every machine has to be programmed with the ballot design, and that programming is copied in by election officials on a USB stick or memory card. If someone can infect that programming, they can spread an attack to the machines and potentially tamper with a fraction of the votes without anyone detecting it.

So what can be done to address this risk?

We need to make sure that every vote is recorded on a piece of paper, too. Without paper, there may be no evidence we can go back and look at that would reveal vote tampering. ballot design are locked down and never accessible from the internet.

What other areas beyond voting machines are vulnerable?

Voter registration systems connected to the internet are a major concern. In 2016, one of the most worrying cyber attacks was Russian attempts to probe,. We also need to worry about electronic poll books that many states use to check voters in on Election Day. This equipment is often networked, and if it fails it could lead to chaos at the polls.

How can we bolster defenses here? The main thing is to apply the same good security practices developed for protecting other government and industry databases. We also need to have backup procedures in place in case the technology fails.

Auditing results can catch vote manipulation. Are post-election audits in the US sufficiently robust?

No. Some states don't check ballots at all; others examine them in a fixed We need "risk-limiting" audits. Here you agree in advance the probability you're willing to tolerate of an election outcome being manipulated and not detected. You then look at enough paper ballots so the odds of someone getting away with fraud are lower than the target percentage.

Why don't we have these audits everywhere?

States have been slow to adopt new ways of countering cyberthreats. Fortunately, risk-limiting audits don't have to be particularly expensive. When an election isn't close, you might to confirm the result with high statistical confidence by examining a few hun dred ballots across a state; in extremely close elections, you often have to do an automatic recount anyway.

Would it be better if the US had a fed erally mandated, nationwide voting system rather than many different state and local ones?
It might be easier to secure a single, uni fied voting system, but election admin istration in the US is the responsibility of state and local governments, and I don't see that changing soon. What we can do is to set national standards for election cybersecurity that states should meet or exceed.

Could one tie federal money for secur ing elections to the adoption of those standards at the state level?
That could be quite effective, and there's a bipartisan draft bill in Congress called the Secure Elections Act that would do just that.

What would have to happen for online voting. Estonia-style, to become broadly viable in the US?
Online voting carries extremely big risks. You need to protect internet connected servers running the elec tion from sophisticated adversaries and protect voters' own devices from mal ware. That's why Estonia is the only country where national elections are largely online, and its system is unlikely to withstand a concerted attack. It may be decades before we're able to secure online systems to the same level we expect from voting in polling places today.

Some people have floated the idea of blockchain-based voting systems. Are you a fan?
Blockchain doesn't fix the hard parts of securing online elections. It's just another form of recording votes. If attackers compromise voters' devices or the servers that record votes and log them to the blockchain, they can still manipulate election outcomes. There are no easy solutions here.

Here’s how hackers could cause chaos in the US midterm elections

In the months leading up to November's mid- term elections in the US, hordes of foreign hackers will head to their keyboards in a bid to influence the outcome. Their efforts will include trying to get inside the digital infrastructure that supports the electoral process.
There's a worrying precedent here. Last year. the Department of Homeland Security (DHS) notified 21 states that Russia had targeted their election systems in the months leading up to t
he 2016 presidential election.
DHS officials said the Russians were mainly scanning computers and networks for security holes rather than taking advantage of any flawes they discovered. Still, that's no cause for com placency. Intelligence officials are already warn ing that Russia is intent on meddling in this year's midterm elections, too-and most of the digital technology that will be used predates the launch of the first iPhone in 2007. Here's what cyberattackers might target.

T

check-in

Voter registra-

Voter

Vote tallying

Voting

tion systems

and reporting machines

THE TECHNOLOGY: In many states, precinct poll work ers use tablet-like electronic poll books, rather than paper ones, to verify voters. These machines are often networked to one another and run tailor made software.

THE RISKS: Hackers could target the networks to gain access to poll books, either shutting them down or altering data that's on them. They could also break into the systems of companies that develop soft-ware for the poll books and insert malicious code.

Compromising poll books could cause chaos during an elect

THE TECHNOLOGY: These sys tems keep a digital record of authorized voters, and data from them populates "poll books" used to check people in at precinct polling stations.

THE RISKS: Many voter registration systems are old

a report last year by the BrennanCenter for Justice at NewYork University School of Law estimated that 41 states were still using ones built at least a decade ago. They are hosted on servers and need connectivity to receive voter data and transfer it to poll books. Hackers who gain ac -cess to them could erase voters' entries or create fictitious ones and then mail in votes for the fake personas. That could tip the balance in tight races.

THE TECHNOLOGY: The US uses two main types of electronic voting machines. Optical-scan ballot readers scan and record paper ballots filled in by voters, while direct-recording elec tronic, or DRE, machines display ballot options on a screen and record voters' choices electronically. Only some DRE machines produce paper records too.

THE RISKS: Voting

machines are programmed with the ballot design, which includes names of the races and candidates involved. The design is set up on

THE TECHNOLOGY: The soft- ware managing vote tallying and reporting typically runs on computers using standard operating systems.

THE RISKS :Hackers could tar- get the software to throw doubt on the outcome of elec- tions. While this may sound unilkely, there are strong sus picions Russian hackers were behind an attack that deleted key files from the Ukrainian central election commission's system in a 2014 vote.

Beyond all these risks, plenty of other nightmare sce iarios could affect the

ion. For instance, voters may be

This makes the systems

election management different stages

told that they've already voted when in fact they haven't. Ideally, all polling stations should have backup plans in place that allow them to print provisional ballots if the machines fail.

tempting targets. In his indict ment of 12 Russian hackers In July, US special counsel Robert Mueller alleged that they penetrated the website of one (unnamed) state board of elections in 2016 and stole partial Social Security num bers, driver's license numbers, and other data for around halfa million votors.

systems at a central election office or a vendor. The infor mation is typically then trans- ferred to each machine by officials using memory cards or USB keys. Paperless machines are still used in 13 states, and five rely solely on them.

reviewed .They include distributed denial of service attacks, which knock web-connected systems out of action by flooding them with fake traffic, and ran- somware attacks, which use malware to encrypt data-or, in the worst case, destroy it.

Kenya's technology evolved. Its political problems stayed the same.

Long before the internet, hate speech flourished in echo chambers of a different kind.

By **Nanjala Nyabola**

In 2007, incumbent Mwai Kibaki won a divisive presidential election in Kenya. Street protests escalated to ethnic violence in parts of the country, and by April 2008 more than 1,500 people had been killed. A decade later, another election also featured widespread allegations of fraud, and more violence. The casualties were lower this time, but just over 100 were killed, almost all by the police in opposition strongholds.

Technology and politics are inextricably linked in Kenya, in part because technology was proposed as the solution to the structural issues that led to the violence following the 2007 election. The Independent Review Commission established in 2008 argued that technol ogy would help bridge the trust gap between key politi cal actors and protect the autonomy of the bureaucracy surrounding elections. In line with the commission's recommendations, voter registration, voter identifica tion, and vote tallying are all nominally computerized. These efforts culminated in the 2017 election, which was supposed to be Africa's first fully digital election.

That they didn't work is a lesson in what technology can and cannot fix in politics. Perhaps the primary lesson is that when communication platforms cater to specific audiences while shutt- ing out others amid existing social divides, hate speech thrives. And this was as true of pre internet technology as it is now.

Twenty-five years ago, Kenya had one state-owned radio and television broad caster, but by 2017 there were over 60 licensed television stations and 178 radio stations. Kenya has two official languages English and Kiswahili- As part of the democratization process in the 1990s, local language radio stations were encouraged as way to bring more people into the national conversa- tion while preserving regional cultures.

The unexpected result But it turns out that local-language radio stations are particularly vulnerable to becoming channels for hate speech. They function as closed systems shielded from scrutiny by institutions that don't have the capacity to manage them, or any interest in doing so. By the time the threat inherent in these stations was identified. it had already materialized, and regulators are still playing catch-up. Kenya has laws prohibiting hate speech in media and numerous bodies ostensibly working against it, but as late as July 2017, the National Integration and Cohesion Commission was warning that Kameme FM, a Kikuyu-language radio station owned by Kenyan president Uhuru Kenyatta, was responsible for the most incidents of hate speech related to the election. Despite this finding, the station received no public censure.

Technology has changed radically in Kenya over the past decade, as it has everywhere else. Almost nine out of 10 people have a mobile phone, and a quarter of the homes have an Internet con- nection-among the highest rates in the developing world. In a population of about 48 million, there are at least seven million Kenyan Facebook accounts and another 10 million on WhatsApp. Twitter lags behind at only a million accounts, but

Nanjala Nybola is the author of Digital Democracy. Analogue Politics:How the Internet Era Is transforming Kenya.

In 1955, science fiction writer Isaac Asimov published a short story about an experiment in "electronic democracy," in which a single citizen, selected to represent an entire population, responded to questions generated by a computer named Multivac. The machine took this data and calculated the never needed to happen. Asimov's story was set in Bloomington, Indiana, but today an approximation of Multivac is being built in China.

For any authoritarian regime, "there is a basic problem for the center of figuring out what's going on at lower levels and across society," says Deborah Seligsohn, a political scientist and China expert at Villanova University in Philadelphia. How do you effectively govern a country that's home to one in five people on the planet, with an increasingly complex economy and society, if you don't allow public debate, civil activism, and electoral feedback? How do you gather enough information to actually make decisions? And how does a government that doesn't invite its citizens to participate still engender trust and bend public beh- avior without putting police on every doorstep?

Hu Jintao, China's leader from 2002 to 2012, had atte- mpted to solve these problems by permitting a modest democratic thaw, allowing avenues for grievances to reach the ruling class. His successor, Xi Jinping, has reversed that trend. Instead, his strategy for understanding and respond- ing to what is going on in a nation of 1.4 billion relies on a combination of surveillance, Al, and big data to monitor people's lives and behavior in minute detail.

It helps that a tumultuous couple of years in the world's democracies have made the Chinese political elite feel increasingly justified in shutting out voters. Developments such as Donald Trump's election, Brexit, the rise of far right parties across Europe, and Rodrigo Duterte's reign of terror in the Philippines underscore what many critics see as the problems inherent in democracy, especially populism, instability, and precariously personalized leadership.

Since becoming general secretary of the Chinese Communist Party in 2012, Xi has laid out a raft of ambitious plans for the country, many of them rooted in technology including a goal to become the world leader in artificial intelligence by 2030. Xi has called for "cyber sovereignty" to enhance censorship and assert full control over the domestic internet. In May. he told a meeting of the Chinese Academy of Sciences that technology was the key to achieving "the great goal of building a socialist and modernized nation." In January, when he addressed the nation on television, the bookshelves on either side of him contained both classic titles such as Das Kapital and a few new additions, including two books about artificial intel ligence: Pedro Domingos's The Master Algorithm and Brett King's Augmented: Life in the Smart Lane. "No government has a more ambitious and far-reaching plan to harness the power of data to change the way it governs than the Chinese government." says Martin Chorzempa of the Peterson Institute for International Economics in Washington, DC. Even some foreign observers, watching from afar, may be tempted to wonder if such data-driven governance offers a viable alternative to the increasingly dysfunctional-looking electoral model. But overrelying on the wisdom of technology and data carries its own risks.

Data instead of dialogue

Chinese leaders have long wanted to tap public senti ment without opening the door to heated debate and criticism of the authorities. For most of imperial and modern Chinese history, there has been a tradition of disgruntled people from the countryside traveling to Beijing and staging small demonstrations as public "petitioners." The thinking was that if local authorities. didn't understand or care about their grievances, the emperor might show better judgment.

Under Hu Jintao, some members of the Communist Party saw a limited openness as a possible way to expose and fix certain kinds of problems, Blogs, anticorruption journalists, human rights lawyers, and online critics 1 spot lighting local corruption drove public debate to ward the end of Hu's reign. drove public debate to ward the end of Hu's reign. petpetitioners have come to the capital to draw attention to scandals such as illegal land .seizures by local authorities and contaminated milk powder.

But police are increasingly stopping petitioners from ever reaching Beijing. "Now trains require national IDs to purchase tickets, which makes it easy for the authorities to identify potential 'troublemak ers' such as those who have protested against the government in the past,"identify potential 'troublemak- ers' such as those who have protested against the government in the past," says Maya Wang, senior China researcher for Human Rights Watch. "Several petitioners told us they have been stopped at train platforms." The bloggers, activists, and lawyers are also being systematically silenced or imprisoned, as if data can give the government the same informa tion without any of the fiddly problems of freedom. The idea of using network technology as a tool of governance in China goes back to at least the mid-1980s. As Harvard political scientist JulianGewirtz explains, "When the Chinese government saw that informa- tion technology was becoming a part of daily life, it realized it would have a powerful new tool for both gathering controlling culture, for making Chinese people more 'modern' and more 'governable' which have been perennial obsessions of the leadership " Subsequent

As far as we know, there is no single master blue print linking technology and governance in China. But there are several initiatives that share a common strategy of harvesting data about people and companies to inform decision-making and create systems of incentives and punishments to influence behavior. These initiatives include the State Council's 2014 "Social Credit System," the 2016 Cybersecurity Law, various local-level and private enterprise experiments

government agencies, People on the list have found themselves blocked from borrowing money, booking flights, and staying at luxury hotels. China's national transport companies have created additional blacklists, to punish riders for behavior like blocking train doors or picking fights during a journey; offenders are barred from future ticket purchases for sie or 12 months. Earlier this year, Reijing debuted a series of blacklists to prohibit "dishonest" enterprises from being awarded future gov ernment contracts or land grants,

A few local governments have experi mented with social-credit "scores," though it's not clear if they will be part of the national plan. The northern city of

Top:In the city of Xiangyang, cameras linked to face recognition
technology
project photos of jaywalkers, with names and ID numbers, on a billboard.

in "social credit," "smart city" plans, and technology driven policing in the western region of Xinjiang. Often ha they involve partnerships between the government i and China's tech companies.

The most far-reaching is the Social Credit System, th though a better translation in English might be the th "trust" or "reputation" system. The government plan, e which covers both people and businesses, lists among its goals the "construction of sincerity in government affairs, commercial sincerity, and judicial credibility"

("Everybody in China has an auntie who's been swin- dled. There is a legitimate need to address a break- down in public trust," says Paul Triolo, head of the geotechnology practice at the consultancy Eurasia Group.)

To date, it's a work in progress, though various pilots preview how it might work in 2020, when it is supposed to be fully implemented.

Blacklists are the system's first tool. For the past five years, China's court system has published the names of people who haven't paid fines or complied with judgments. Under new social-credit regula tions, this list is shared with various businesses and

.

Rongcheng, for example, assigns a score to each of its 740,000 residents, *Foreign Policy* reported. Everyone begins with 1,000 points. If you donate to a charity or win a government award, you gain points: if you violate a traffic law, such as by driving drunk or speeding through a crosswalk, you lose points. People with good scores can earn discounts on winter heating supplies or get better terms on mortgages; those with bad scores may lose access to bank loans or promotions in government jobs. City Hall showcases posters of local role models, who have exhibited "virtue" and earned high scores.

"The idea of social credit is to monitor and manage how people and institutions behave," says Samantha Hoffman of the Mercator Institute for China Studies in Berlin."But they're not all connected in the same way-there's no overarching plan," Hoffman points out.

"Once a violation is recorded in one part of the system, it can trigger responses in other parts of the system. It's a concept designed to support both economic development and social management, and it's inherently political.

" Some parallels to parts of China's blueprint already exist in the US: a bad credit score can prevent you from taking out a home loan, parts of China's blueprint already exist in the US: a bad credit score can prevent you from taking out a home loan, while a felony conviction suspends or annuls your right to vote, for example. "But they're not all connected in the same way-there's no overarching plan," Hoffman points out.

One of the biggest concerns is that because China lacks an independent judiciary, citizens have no recourse for disputing false or inaccurate allegations. Some have found their names added to travel blacklists without notification after a court decision. Petitioners and investigative journalists are monitored according to another system, and people who've entered blacklists without notification after a court decision. Petitioners and investigative journalists are monitored according to another system, and people who've entered drug rehab are watched by yet a different monitoring system.

"Theoretically the drug user databases are supposed to erase names after five or seven years, but I've seen lots of cases where that didn't happen," says Wang of Human Rights Watch. "It's immensely difficult to ever take yourself off any of these lists."

Occasional bursts of rage online point to public resentment, News that a student had been turned down by a college because of her father's inclusion on a credit blacklist recently lit a wildfire of online anger. The college's decision hadn't been officially sanctioned or ordered by the government. Rather, in their enthusiasm to support the new policies, school administrators had simply taken them to what they saw as the logical conclusion.

The opacity of the system makes it difficult to evaluate how effective experiments like Rongcheng's are. The party has squeezed out almost all critical voices since 2012, and the risks of challenging the system-even in relatively small ways have grown. What information cal voices since 2012, and the risks of challenging the system-even in relatively small ways have grown. What information is available is deeply flawed: systematic falsification of data on everything from GDP growth to hydropower use pervades Chinese government statistics. Australian National University researcher Borge Bakken estimates that official crime figures, which the government has a clear incentive to down- play, may represent as little as 2.5 percent of all criminal behavior. In theory, data-driven governance could help fix these issues-circumventing distortions to allow the central government to gather information directly. That's been the idea behind, for instance, introducing air-quality monitors that send data back to central

In theory, data-driven governance could help fix these issues circumventing distortions to allow the central government to gather information directly, That's been the idea behind, for instance, introducing air quality monitors that send data back to central authorities rather than relying on local officials who may be in the pocket of polluting industries. But many aspects of good governance are too complicated to allow that kind of direct monitoring and instead rely on data entered by those same local officials.

However, the Chinese government rarely releases performance data that outsiders might use to evaluate these systems. Take the cameras that are used to iden- tify and shame jaywalkers in some cities by projecting their faces on public billboards, as well as to track the prayer habits of Muslims in western China. Their accu- racy remains in question particular, how well can facial-recognition software trained on Han Chinese Algo faces recognize members of Eurasian minority groups? Moreover, even if the data collection is accurate, how Writin will the government use such information to direct or thwart future behavior? Police algorithms that predict who is likely to become a criminal are not open to public scrutiny, nor are statistics that would show whether crime or terrorism has grown or diminished. (For example, in the western region of Xinjiang, the available information shows only that the number of people taken into police custody has shot up dramatically, rising 731 percent from 2016 to 2017.)

" It's not the technology that created the policies, but technology greatly expands the kinds of data that the Chinese government can collect on individuals," says Richard McGregor, a senior fellow at the Lowy Institute and the author of The Party: The Secret World of China's Communist Rulers. "The internet in gChina acts as a real-time, privately run digital inteligence service."

"Algorithmic policing

Writing in the *Washington Post* earlier this year ,Xiao Qiang,a professor of communications at the

In the city of Xiangyang,
cameras
linked to face recognition technology project photos of jaywalkers, with names and ID
numbers, on a billboard.